دراسات عالمية

Panton 116 C



استخبارات وسائل التواصل الاجتماعي

السير ديفيد أوماند، وجيمي بارتليت، وكارل ميلر

تصوير

أحمد ياسين



مركز الإمارات للدراسات والبحوث الاستراتيجية

العدد 125



استخبارات
وسائل التواصل الاجتماعي

مركز الإمارات للدراسات والبحوث الاستراتيجية

أنشئ مركز الإمارات للدراسات والبحوث الاستراتيجية في أبوظبي بتاريخ 14 آذار/ مارس 1994؛كمؤسسة بحثية مستقلة تعنى بدراسة القضايا الاستراتيجية السياسية والاقتصادية والاجتماعية والمعلوماتية، التي تهم دولة الإمارات العربية المتحدة ومنطقة الخليج العربي خصوصاً والعالم العربي عموماً، ومتابعة أهم المستجدات الإقليمية والدولية.

وفي إطار التفاعل الثقافي والتعاون العلمي، يصدر المركز سلسلة **دراسات عالمية** التي تعنى بترجمة أهم الدراسات والبحوث التي تنشر في دوريات عالمية مرموقة، وتتصل موضوعاتها باهتمامات المركز العلمية، كما تهتم بنشر البحوث والدراسات بأقلام مشاهير الكتاب ورجال السياسة. ويرحب المركز بتلقي البحوث والدراسات المترجمة، وفق قواعد النشر الخاصة بالسلسلة.

رئيس التحرير: **أمل عبدالله الهدّابي**

تصوير

أحمد ياسين

دراســات عـالميـــة

استخبــارات
وسائـل التواصـل الاجتماعي

السير ديفيد أوماند، وجيمي بارتليت، وكارل ميلر

العـدد 125

تصـدر عـن



مركـز الإمـارات للدراسـات والبحـوث الإسـتـراتيجيـة

محتوىٰ الدراسة لا يعبر بالضرورة عن وجهة نظر المركز

This is an authorized translation of "Introducing Social Media Intelligence," by Sir David Omand, Jamie Bartlett & Carl Miller; and published by *Intelligence and National Security* vol. 27, no. 6 (December 2012): 801–823. The ECSSR is indebted to the authors and original publisher for permitting the translation, publication and distribution of the above title under its name.

الطبعة الأولى 2014

ISSN 1682-1211

النسخـــة العاديـــة ISBN 978-9948-14-848-7

النسخة الإلكترونية ISBN 978-9948-14-849-4

توجه المراسلات باسم رئيس تحرير سلسلة **دراسات عالمية**

على العنوان الآتي:

مركز الإمارات للدراسات والبحوث الاستراتيجية

ص ب: 4567

أبوظبي، دولة الإمارات العربية المتحدة

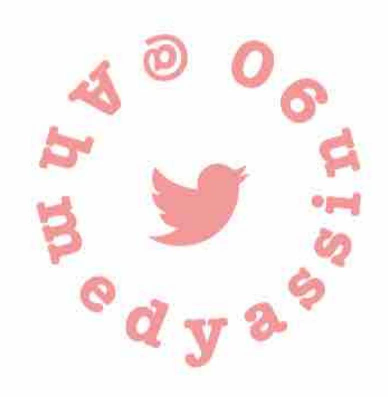
هاتف: +9712-4044541

فاكس: +9712-4044542

E-mail: pubdis@ecssr.ae

Website: http://www.ecssr.ae

المحتويـات


@Ahmedyassin90

ملخص

نقدم في هذه الدراسة أحدث فرع في مجال الاستخبارات؛ فعقب نشوء الاستخبارات التصويرية IMINT، والاستخبارات البشرية HUMINT، واستخبارات الإشارات SIGINT وغيرها، تأتي الآن استخبارات وسائل التواصل الاجتماعي التي تُعرف اختصاراً بـ SOCMINT. ففي عصر باتت تنتشر فيه وسائل التواصل الاجتماعي في كل مكان، ثمة مسؤولية ملقاة على عاتق المجتمع الأمني باعتماد استخبارات وسائل التواصل الاجتماعي ضمن منظومة الاستخبارات الوطنية. ولكن، لا يتعين القيام بذلك إلا بعد اختبارين مهمين: الأول، أن يقوم هذا الفرع من الاستخبارات على أساس منهجي متين فيما يتعلق بعمليات جمع المعلومات، والإثبات، والتحقق، والفهم، والتطبيق. والثاني، هو أن يعالج بصورة مشروعة الخطر الأخلاقي الذي تنطوي عليه نشاطات استخبارات وسائل التواصل الاجتماعي. وتقدم هذه الدراسة إطار عمل لكيفية تحقيق ذلك.

مقدمة

في يوم الخميس الموافق 4 أغسطس 2011، أطلق شرطي بريطاني النار على مارك دوجان في منطقة توتنهام فأرداه قتيلاً، وفي صباح اليوم السادس من الشهر نفسه أظهرت قنوات التواصل الاجتماعي عداوة متزايدة تصاحبها تهديدات صريحة ضد الشرطة. وبداية من اليوم السابع أشارت المعلومات المستقاة من وسائل التواصل الاجتماعي إلى احتمال انتشار الفوضى إلى أجزاء أخرى من لندن ثم إلى إنجلترا. وعلى مدار الأيام القليلة التالية تنامى المحتوى الذي يشير إلى النيات أو الأعمال الإجرامية بنسب هائلة عبر كل من شبكات التواصل الاجتماعي المفتوحة المصادر مثل تويتر، والشبكات المغلقة مثل خدمات الرسائل الفورية لأجهزة بلاكبيري، والمجموعات المغلقة مثل منتديات الدردشة. وعلى نحو مشابه، كان هناك عدد هائل من الرسائل تسعى لتقديم معلومات للشرطة، إما بشأن اندلاع الفوضى وإما بشأن هويات الأشخاص الذين يقفون خلفها.[1]

في أعقاب ذلك اعترف مسؤولو الشرطة بأنهم لم يكونوا مُجهّزين على نحو كاف لجمع المعلومات الاستخبارية عبر وسائل التواصل الاجتماعي. وقال أحد المتخصصين في مجال الاستخبارات إن الأمر كان أشبه «بالبحث في المكتبة البريطانية عن صفحة في كتاب من دون فهرست يمكن الاسترشاد به».[2] ذلك أن وسائل التواصل الاجتماعي لم تناسب النظُم التي تستخدمها الشرطة في تلقي المعلومات والتحقق منها وتحديد الأولويات ونشرها، ومن ثم لم تتم الاستفادة منها على النحو السليم. وقد أشار كبير مفتشي الشرطة الملكية إلى أنه «على رغم وجود بعض الاستثناءات الفردية الملحوظة، لا يتم فهم قوة هذا النوع من الوسائل (سواء ما يتعلق بإرسال المعلومات أو تلقيها) ولا إدارته بشكل جيد».[3] وخلص إلى أن «هناك كثيراً من الأشياء التي يتعين على الشرطة تعلمها بشأن وسائل التواصل الاجتماعي، ووسائل الاتصال الحديثة التي تتطور بسرعة في هذه الأيام».[4]

منذ ذلك الوقت تحركت الحكومة البريطانية للتعامل مع هذا المجال الجديد؛ فأسست شرطة العاصمة مركزاً لوسائل التواصل الاجتماعي خاصاً بدورة الألعاب الأولمبية في أثناء فعالياتها بلندن. ويُعتقد أن عدداً من أجهزة الشرطة في المملكة المتحدة ومناطق أخرى تختبر أنواعاً مختلفة من البرامج الآلية التي تجمع محتوى وسائل التواصل الاجتماعي وتحلله؛ بهدف جمع المعلومات للمساعدة في التحقيقات الجنائية، وجس نبض المجتمعات التي يعمل فيها المجرمون.[5] واستخدمت الشرطة برنامج فليكر Flickr لجمع معلومات حول هويات المشتبه فيهم من خلال الصور. وأطلق مركز العلوم والتكنولوجيا للفضاء الإلكتروني والتأثير Cyber and Influence Science and Technology Centre التابع لوزارة الدفاع في المملكة المتحدة دعوات لإجراء أبحاث تهدف إلى تطوير مجموعة من القدرات، بما في ذلك «تقدير حالة الفضاء الإلكتروني» و«التأثير عبر الفضاء الإلكتروني» و«مراقبة وسائل التواصل الاجتماعي وتحليلها» و«الاستعانة بمجموعة كبيرة من المصادر عبر الإنترنت».[6]

وتقف خلف هذه التطورات استثمارات عامة مزمعة وقدرات كبيرة من المنتظر أن تتيح للسلطات الاستمرارية في الوصول إلى البيانات الخاصة بوسائل الاتصالات

والحصول - بموجب إذن عند الضرورة - على محتوى الاتصالات التي تجري عبر الإنترنت، بما في ذلك وسائل التواصل الاجتماعي. وقد تم في المملكة المتحدة اقتراح تشريع جديد لضمان التزام وكالات إنفاذ القانون بالقدرة على التعامل مع الجريمة والإرهاب في ظل استخدام المجرمين للوسائل التقانية الحديثة والطرائق الجديدة في التواصل في الفضاء الرقمي للتخطيط للجرائم وتنفيذها.

ويثير الاهتمام السريع لسلطات إنفاذ القانون بالمعلومات الاستخبارية المستقاة من وسائل التواصل الاجتماعي (التي نطلق عليها مصطلح استخبارات وسائل التواصل الاجتماعي) أسئلة بشأن الإطار المنهجي والأخلاقي الذي سوف تستخدم فيه مثل تلك المعلومات. إلى ذلك، يشكل القبول الشعبي ركيزة أساسية في أي شكل من نشاطات جمع المعلومات الاستخبارية، ويمكن تأمين هذا القبول الشعبي فقط إذا تم استخدام استخبارات وسائل التواصل الاجتماعي بشكل سليم، وإذا تم منح الصلاحيات الخاصة للقيام بذلك على نحو سليم أيضاً. وتعرض الدراسة إطار عمل لكيفية تحقيق ذلك.

عصر وسائل التواصل الاجتماعي

نعيش اليوم في عصر وسائل التواصل الاجتماعي. إن الفيسبوك وتويتر وجوجل ولينكيدإن، جميعها أمثلة على التحول السريع في حياة الناس، في التفاعلات والهويات والنقاشات والآراء، إلى ساحة جديدة يختلط فيها العام بالخاص، وإلى مشاع اجتماعي رقمي واسع. ويجري هذا التحول على نطاق واسع وغير مسبوق. لك أن تعرف أنه في الفيسبوك وحده، تجري إضافة 250 مليون صورة يومياً،[7] وكذلك تضاف 200 مليون تغريدة إلى تويتر،[8] وأربعة مليارات مشاهدة فيديو يومياً على يوتيوب.[9]

في الوقت الذي يقوم فيه مزيد من الناس بتحويل حياتهم إلى منصات وسائل تواصل اجتماعي، فإنهم يصبحون جزءاً من الساحة العامة على نحو متزايد، ومن ثم يصبحون ذوي أهمية إلى الهيئات العامة التي تقوم باستغلالهم. ولاشك في أن فهم محتوى وسائل التواصل الاجتماعي يعطي الهيئات العامة فرصةً لفهم الجمهور الذي تخدمه والاستجابة له بشكل أفضل. فعلى سبيل المثال، يعكف خبراء الصحة العامة على الاستفادة من فحص

التغريدات وبحث الطلبات ليتمكنوا من تحديد الأوبئة بسرعة أكبر مما يمكن فعله في حال استخدام الطرق التقليدية.[10] ويعتقد علماء النفس في الولايات المتحدة الأمريكية أن الفيسبوك يحتوي على مؤشرات قيمة بشأن الصحة العقلية، ويبدو فعلياً أن السجلات الشخصية (البروفايلات profiles) الخاصة بوسائل التواصل الاجتماعي لعدد من المشاركين في حوادث إطلاق نار في المدارس، مثل المشتبه فيه في حادث إطلاق النار في مدرسة بولاية أوهايو، تي جيه لين T.J. Lane، تقدم بعض المحتوى الإرشادي الذي لا يخلو من دلالة.[11] وتعتقد الأمم المتحدة أن الاستفادة من وسائل التواصل الاجتماعي يمكن أن تساعد على معالجة البطالة العالمية وانعدام الأمن الغذائي.[12]

إضافة إلى ذلك، غدت ساحات وسائل التواصل الاجتماعي الآن تمثل أهمية متنامية للأمن والسلامة العامة. فقد استخدم الفيسبوك في محاولة لتأجير قتلة محترفين، ويستخدمه مشتهو الأطفال لإغواء أهدافهم، وانتهاك الأوامر التقييدية، وسرقة الهويات، وترهيب الضحايا عبر الإنترنت.[13] ويشار هنا إلى أن حركة الشباب المجاهدين في الصومال التابعة لتنظيم القاعدة تدير حساباً على تويتر، في حين يستخدم القراصنة الذين ينشطون في خليج عدن المدونات وتويتر والفيسبوك في التخطيط لعملياتهم والتنسيق فيما بينهم.[14] وقد أوردت صحيفة ذا ديلي ميل The Daily Mail أن هناك 12300 جريمة مزعومة ترتبط بالفيسبوك في عام 2011.[15]

عندما يطور المجتمع ويتبنى أساليب جديدة للتواصل والتنظيم، مثل وسائل التواصل الاجتماعي، يصبح لدى المؤسسات العامة، بما في ذلك أجهزة الشرطة والاستخبارات، مسؤولية للتعامل والتكيف معها. ويبدو أن الانتشار الهائل لوسائل التواصل الاجتماعي ما هو إلا أحدث حلقة في سلسلة طويلة من الابتكارات التقانية المزعجة، وهو أمر يستدعي أن تقوم السلطات الآن بدروها في التعامل معه.

استخبارات وسائل التواصل الاجتماعي: فرص وفوائد

يحمل قياس وفهم وجوه ملايين الناس الذين يتحاورون ويتحادثون ويمزحون ويشجبون أشياء ويستحسنون أخرى بطريقة رقمية، قيمةً كبيرة لكثير من المجالات

والشؤون والصناعات. وتتوافر حالياً مجموعة من البرامج الخاصة بـ"البيانات الضخمة" Big Data التي تهدف إلى فهم وسائل التواصل الاجتماعي والاستفادة منها. تشكل هذه الأدوات، التي تُعرف باسم تحليلات وسائل التواصل الاجتماعي، طيفاً واسعاً ومتنوعاً يراوح بين المعلنين الذين يرصدون إشاعات وسائل التواصل الاجتماعي بهدف تتبع التوجهات التي تتعلق بمنتجاتهم، والشركات التي ترصد سمعتها عبر وسائل التواصل الاجتماعي، إلى رصد خرائط العلاقات الاجتماعية بين الناس، إلى استقاء "الحكمة من جمهور الناس" فيما يتعلق بالحلول الممكنة في حالات الطوارئ، إلى إجراء تحليل لغوي للمشاركات التي ترسل عبر المنتديات وتحليل الشبكات لمستخدمي تويتر. وقد استخدمت جهود أكاديمية أولية وسائل التواصل الاجتماعي لتعزيز الاستثمارات في صناديق الاستثمارات العالية المخاطر.[16]

وبالنظر إلى تقنيات استخبارات وسائل التواصل الاجتماعي المتوافرة الآن – وكذلك التهديدات التي تواجهنا حالياً – يمكن للقدرات التالية أن تساهم، على سبيل المثال، في تحقيق الأمن العام في المستقبل:

- **المعلومات التي يتم استقاؤها من مصادر الجمهور**: يمكن أن تساعد هذه على ضمان تدفق أفضل للمعلومات بين المواطنين والحكومة، ولاسيما في حالات الطوارئ.[17] فمن خلال الدخول إلى وسائل التواصل الاجتماعي، يمكن أن يصبح المُتفرّجون السلبيون مواطنين صحفيين نشطين، يقدمون المعلومات وينقلونها من مواقع الحدث مباشرة. فعلى سبيل المثال، أشار تقرير إدارة تفتيش الشرطة الملكية في بريطانيا حول أحداث الشغب التي تتم مراقبتها، إلى تأسيس خدمة خاصة بالرسائل على الموقع الإلكتروني لشرطة ويست ميدلاندز، والتي أتاحت للمواطنين إرسال رسائل وطرح أسئلة تساعد الشرطة على تكوين صورة للموقف على الأرض في الوقت المطلوب، كما تسمح للناس بتحديد صور المشتبه فيهم حيث يتم تحميلها على الموقع.[18] وقد أصبحت الاستفادة من "حكمة جمهور الناس" تمثل بالفعل قيمة عظيمة وواضحة. فعلى سبيل المثال، أتاح تطبيق "أوشاهيدي" Ushahidi المفتوح المصدر لجماعات كبيرة من الناس، تقديم شهادة جماعية حول

كل شـيء بداية من زلزال هاييتي إلى الطرق المغلقة في واشـنطن دي سـي.[19] هـذه التطبيقـات المبهـرة مـا هـي إلا البدايـة، وكلـما زادت قـوة الأسـاليب المسـتخدمة للاستفادة من مثل هذا النوع من المعلومات، من حيث النطاق والديناميـة، ازدادت فاعلية الاستجابات التي يمكن القيام بها، ابتداء من تقـديم كاسـحات للثلـوج إلى التزويد بمياه الشـرب.

- **البحث والفهم**: إن البحث المعتمد على وسـائل التواصـل الاجتماعـي قـد يسـاهم في فهمنا لعدد من الظـواهر. وقـد يشـمل ذلـك قيـاس مسـتويات العنـف ومؤشـراته والظروف التي تسمح به، والسُبل التي تقود للتشدد، وتحليل كيفيـة تَشَّـكُل الأفكـار وتغيّرها، والتحقيق في التفـاعلات الاجتماعيـة-التقانيـة بـين الأشـخاص المتصـلين بالإنترنت وغير المتصلين به. ودون المستوى التكتيكي والعملياتي، يمثل فهم الخلفيـة العامة للأشخاص أهمية كبيرة للعمل الأمني. على سـبيل المثـال، تهـدف اسـتراتيجية مكافحة الإرهاب البريطانيـة إلى تقلـيص التهديـدات الناشـئة عـن الإرهـاب حتـى يستطيع الناس ممارسة حياتهم العادية، بحرية وثقة، ويُعتقـد أن الطريقـة للقيـام بهـذا على المدى الطويل تكون من خلال معالجة الأسباب الأساسية الاجتماعيـة والفكريـة والسياسية للإرهاب.

إضافة إلى ذلك، تقدم زيادة استخدام وسائل التواصل الاجتماعي، مع النمو السـريع لمناهج التحليل حالياً فرصة جديدة لسلطات إنفاذ القـانون لجمـع معلومـات اسـتخبارية عملياتية يمكن أن تساعدها على تحديد النشاط الإجرامي، وتقديم تحذيرات مبكرة حـول موجـات الاضـطرابات، وبيانـات ومعلومـات اسـتخبارية حـول الجماعـات والأفـراد، والمساعدة على فهم المخاوف الشعبية والتفاعل معها. ويمكن الوصول إلى بعض ذلك عبر المعلومات ذات المصادر المفتوحة التي تُسـتقى مـن تـويتر وغيرهـا مـن محتويـات وسـائل التواصل الاجتماعي التي يُسمح للعامة بالوصول إليها. ويتطلب بعضها الآخـر الحصـول على تفويض قانوني لتجاوز إعدادات الخصوصية والتشفير لمثل هذه التطبيقـات. ويمكـن تلخيص مزايا الاستغلال العملياتي هذا في الآتي:

- **تقدير الموقف في الوقت الحقيقي تقريباً**: هذه هي القدرة على جمع وسائل التواصل الاجتماعي وتصنيفها بطريقة توضح تطور الأحداث. لقد أظهر تحليل تطبيق تويتر أنه على الرغم من أن أغلبية الرسائل أرسلت عبره بعد ورود الخبر في إحدى وسائل الإعلام الرئيسية، فإن "تدفقات" التغريدات التي توضح حدثاً مهماً غالباً ما تسبق التقارير الإخبارية التقليدية.[20] وقد يتيح تحليل حركة الرسائل والمشاركات على وسائل التواصل الاجتماعي تحديداً أسرع للأحداث الجارية من تلك التي تتيحها التقارير التقليدية. ومن خلال تطبيق تقنيات تحديد المواقع، يمكن أن يقود هذا – على سبيل المثال – إلى تكوين خريطة متطورة تظهر زيادة في التغريدات المرتبطة بالعنف المحتمل، ما يسهل تنفيذ الاستجابات الطارئة على نحو أكثر سرعة وفاعلية.

- **فهم ثاقب للمجموعات**: يمكن أن يشمل هذا القدرة على التوصل إلى فهم أفضل لنشاطات وسلوكيات مجموعات محددة من تلك التي تهتم بها الشرطة أو وكالات الاستخبارات. وفي ظل وجود تفويض قانوني، يمكن للشرطة استخدام استخبارات وسائل التواصل الاجتماعي لتحديد وكشف "الموضوعات الساخنة" التي تطفو على المحادثات الخاصة بجماعة محددة وكيفية استجابة المجموعة لحدث محدد. من خلال هذه الأساليب وغيرها، قد تبين استخبارات وسائل التواصل الاجتماعي المستويات العامة من السخط في أوساط مجموعة ما، ومخاوفها وموضوعاتها الرئيسية التي تُحرّك المناقشات داخل المجموعة. وعلى مستوى أعلى من ذلك، يمكن أيضاً تحديد معلومات واستخلاصها فيما يتعلق بالآتي: مواعيد تخطيط المجموعة لمظاهرات أو تجمعات مفاجئة قد تقود إلى عنف أو زيادة التوترات المجتمعية، وتجمعات مشجعي كرة القدم التي قد تتسبب في اضطرابات اقتصادية كبيرة، والمجموعات التي تخطط لتنظيم مظاهرات مضادة والتي قد تغير نوع الحماية الشرطية اللازمة لحفظ الأمن والنظام العام.

- **تحديد النيات الإجرامية أو العناصر الإجرامية في سياق السعي لمنع الجريمة وملاحقة مرتكبيها**: يمكن لسلطات إنفاذ القانون أن تستخدم المراقبة، على النحو الذي يكفله القانون، لاستخدام وسائل التواصل الاجتماعي من قبل الأفراد المشتبه في تورطهم في

جرائم أو مؤامرات إجرامية، والتحقق من حسابات مثل هؤلاء الأفراد، وتحديد الشركاء في الجريمة، وكشف الهويات المنتحلة، وتحديد الشبكات الإجرامية التي تعمل عبر مواقع التواصل الاجتماعي، وتقديم محتوى وسائل التواصل الاجتماعي الذي يشتبه في كونه دليلاً على جريمة ما للنيابة العامة.

تشير مثل هذه الإمكانيات إلى أن استخبارات وسائل التواصل الاجتماعي تستحق أن تحتل مكانة مهمة في منظومة عمل الاستخبارات الوطنية. ومع ذلك، كلما ظهر شكل جديد من الوسائل التقانية، فإنها ستحتاج بعض الوقت حتى يتم تطوير نظُم شرعية وصارمة لرصدها وتحليلها وتفسيرها. وهناك عدد من التحديات الرئيسية التي تحتاج إلى أن تجري معالجتها قبل أن يصبح بالإمكان الاستفادة الكاملة من استخبارات وسائل التواصل الاجتماعي لصالح الأمن القومي والأمن العام. وسنناقش فيما يلي هذه التحديات والحلول المقترحة لها.

تحديات استخبارات
وسائل التواصل الاجتماعي: الضرورة والشرعية

إن الآمال المعلقة على استخبارات وسائل التواصل الاجتماعي بوصفها أداة لإنفاذ القانون، بالإضافة إلى استخدامها بوصفها مصدراً مفتوحاً للمعلومات، يجب أن تُضبط بما يناسب الواقع؛ إذ تعتمد الأساليب التي يتم توظيفها لحماية المجتمع - في النهاية - على شكل من أشكال القبول والمشاركة الشعبية. تدرك استراتيجية الأمن القومي البريطانية أن العمل الأمني والاستخباراتي بشكل عام لا يعتمد على الموافقة والتفهم الشعبي فحسب، بل على الشراكة والمشاركة النشطة من جانب الأفراد والمجتمعات؛ فعندما لا تحظى جهود الدولة بالقبول أو الثقة، يحدث ضرر خطير للأمن.[21]

يمكن الوصول إلى القبول الشعبي والحفاظ عليه من خلال أمرين مهمين: الأول هو أن جمع المعلومات الاستخباراتية قادر على أن يقدم مساهمة فعالة وضرورية تجاه تحقيق السلامة والأمن، والثاني، أن تكون هذه المساهمة متوازنة على نحو يتناسب مع المصالح العامة المرجوة، مثل الحق في التمتع بالحياة الخاصة. وإجمالاً، يتعين أن يسهم النشاط

الاستخباراتي بفاعلية في تحقيق المصلحة العامة، ولا ينتقص منها أو يهدد مصالح أخرى على نحو غير مدروس أو تصعب إدارته. هذه هي تحديات الضرورة والشرعية.

الضرورة

المظهر الأول الذي يتعين أن يقدمه استخدام استخبارات وسائل التواصل الاجتماعي هو أن تكون ناجحة. فإذا لم تكن هناك إمكانية معقولة للمساهمة في تحقيق السلامة العامة، فلن تكون هناك حجة أخلاقية أو مالية لجمع مثل هذه المعلومات أو استخدامها. وإذا لم تكن استخبارات وسائل التواصل الاجتماعي فعالة، فإنها تعرِّض المشتبه فيهم، الذين قد يتضح أنهم أبرياء، للخطر. وقد تنطوي على إلحاق أضرار جانبية بالآخرين الذين يستحقون الرعاية، كما قد تنطوي على خطر إرباك جهود استخباراتية كانت سليمة من دون تدخل تلك الوسائل.

لا يتمثل "نجاح" الاستخبارات في جمع المعلومات أو حتى الأسرار، ولكن في القيمة التي تضيفها على عملية صنع القرار. وفي الواقع، فإن مبرر تأسيس استخبارات وسائل التواصل الاجتماعي - أو أي نوع من الاستخبارات الأخرى - وتطبيقها رغم جميع الأخطار التي قد تنطوي عليها، هو أنها تسهم في تعزيز المصلحة العامة من حيث السلامة والأمن. ولذلك، فهناك ضرورة أخلاقية بأن تقدم عمليات استخبارات وسائل التواصل الاجتماعي فرصة معقولة بكونها ستقود إلى معلومات استخبارية كافية للتدخل، وقابلة للاستخدام بما يسهم في القرارات اللاحقة، مثل تقديم خدمات الطوارئ في المكان المناسب والوقت المناسب.

لكي تعتبر المعلومات "الاستخبارية" ناجحة، يتعين أن تفي بمستويات محددة من حيث كيفية جمعها وتدقيقها والتحقق منها وفهمها وتطبيقها. وقد طورت المصادر المختلفة وأنواع المعلومات طرقاً مميزة لمواجهة هذا التحدي. فعلى سبيل المثال، تقوم استخبارات المصادر المفتوحة OSINT بالاعتماد على ثلاثة مصادر موثوقة؛ فربما تقوم الاستخبارات البشرية HUMINT بدراسة سجل العميل وفحصه، ويتعين على الاستخبارات التصويرية IMINT [التي تجمع المعلومات عن طريق الأقمار الصناعية والصور الجوية]

الانتباه إلى السمات الفنية لمنصة أو وسيلة جمع المعلومات، ويجب على استخبارات الإشارات SIGINT [التي تجمع المعلومات باستخدام الإشارات بين البشر أو الإشارات الإلكترونية] فهم سياق اللغة المستخدمة. وتسعى تقييمات الاستخبارات كافة إلى الحصول على صورة عامة وشاملة على أساس هذه الأنواع المختلفة وعلى موثوقية مساهمتها.

ثمة سمات مميزة يمكن أن تعرف بها استخبارات وسائل التواصل الاجتماعي من خلال فحص كيفية إدماج استخبارات وسائل التواصل الاجتماعي في دورة الاستخبارات التقليدية، ولاسيما الخطوات العملية مثل جمع المعلومات والمعالجة والتحليل والتوزيع.

الوصول إلى البيانات

تمثل "كثرة المعلومات" إحدى الصعوبات التي تواجه استخبارات وسائل التواصل الاجتماعي، وكذلك الحال مع كثير من العمليات الخاصة باستخبارات الإشارات الحديثة. في حين كانت "ندرة البيانات" تمثل المشكلة الرئيسية في جمع المعلومات الاستخبارية السرية خلال الحرب الباردة. وقد تم تفضيل استخدام مصطلح "الوصول" Access على "الجمع" Collection؛ لتوضيح أننا في عالم الإنترنت نتعامل مع عملية مختلفة عن جمع المعلومات الاستخبارية التقليدية. خلال أسبوع الشغب في أغسطس 2011، على سبيل المثال، تم إرسال ملايين الرسائل المتعلقة بأعمال الشغب، وشملت قصصاً إخبارية وشائعات وردود أفعال ومؤشرات على نيات إجرامية.[22] ويعد الأمر المهم في هذه الأحوال هو معرفة ما البيانات التي يتعين الدخول إليها وتحليلها؛ أي فصل الغث عن السمين. إن أسلوب اختبار الأدوات وتصفيتها (بما في ذلك بعض الأساليب مثل البحث الدلالي Semantic Search) متاح، وقد تم استخدامه - على سبيل المثال - بشكل مكثف في استخبارات الإشارات والبحث في رسائل البريد الإلكتروني والكشف القانوني عن الأدلة، وستكون هناك حاجة له في تحليل وسائل التواصل الاجتماعي من قبل سلطات إنفاذ القانون.

تبرز مشكلات مختلفة أخرى أمام المحللين عندما يحاولون استخلاص المعنى العام من مجموعات البيانات الضخمة. وتعد إحدى الطرق المفيدة لمقاربة هذا التحدي هي

الاستفادة من كيفية تعامل الأساليب الكمية التقليدية مع مجموعات البيانات الضخمة. فمعظم المحللين يتجهون إلى تقنية إحصائية لأخذ العينات، حيث تؤخذ كمية من بيانات السكان تمكن إدارتها، وهي تعبر عن الكميات الكبيرة من البيانات التي لا تمكن إدارتها. تعتمد مصداقية وصحة الاستدلالات والاستقراءات التي جرت وفق هذا الأسلوب على الجودة، وبخاصة نسبة تمثيل العينة التي تم جمعها. وقد طور خبراء الإحصاء، على مدار القرن الماضي، أساليب تتيح استخدام مجموعات البيانات الصغيرة بوصفها عينة تمثيلية، ومن ثم تتيح الخروج باستنتاجات أكثر عمومية، ولاسيما من خلال استخدام العينات العشوائية. ببساطة، لا يمكن استخلاص الاستدلالات والاستنتاجات بطريقة معقولة ما لم يكن المرء على دراية بكيفية أخذ العينة وجمع البيانات، حيث يؤثر ذلك كله في الاستنتاجات التي سيجري التوصل إليها.

تكمن المشكلة الرئيسية في أن العلوم الاجتماعية لم تطور بعد منهجاً صارماً لدراسة مجموعات بيانات وسائل التواصل الاجتماعي. وما تم إنجازه هو جهود قليلة فقط لتطوير أنواع مختلفة من طرق أخذ العينات لنظُم البيانات الآلية. وقد تم إيلاء اهتمام أكبر بطرق البحث التي تنتج عينات كبيرة (وهو الشيء الذي تجيده المناهج الحسابية)، أكثر من طرق البحث التي تنتج عينة تمثيلية (وهو الشيء الذي تجيده العلوم الاجتماعية).[23] إضافة إلى ذلك، فإن التطورات المستمرة للتقانة الفائقة التي تعتمد على التطور في علوم الحاسوب في ممارسات أخذ العينات في وسائل التواصل الاجتماعي، لا تحظى باهتمام كبير في أوساط المتخصصين في العلوم الاجتماعية، بما في ذلك نموذج "الانتشار السريع" Forest-Fire (حيث يتم الوصول إلى الروابط والعقد الشبكية node من الخارج بفعل استعلام عشوائي عن معلومة صغيرة لتكوين عينة)، ونشاط المستخدم، والتقنيات التي تعتمد على الموقع.

ليس هناك إلا عدد قليل جداً من البحوث المعتمدة على مجموعات بيانات وسائل التواصل الاجتماعي التي تعترف بأسلوب أخذ العينات التطبيقي، وربما يحد ذلك من النتائج التي يتم التوصل إليها أو يؤثر في تحيزها. تظل الاستراتيجيات المعتادة للحصول على البيانات داخل حقل العمل الأكاديمي الصغير؛ ولكن المتنامي؛ هي ما يطلق عليه عينات "الملاءمة" أو "المصادفة"، ويقصد بذلك أن العينات التي يتم جمعها هي الأكثر

توافراً أو الأسهل وصولاً، وليس الأكثر تمثيلاً.[24] ولأسباب بديهية، فإن هذا الأسلوب في أخذ العينات يقلل من قوة الاستنتاجات التي يتم التوصل إليها. أحد الأمثلة البارزة في هذا الصدد هو الدراسة التي صدرت مؤخراً تحت عنوان **قراءة في أعمال الشغب** ***Reading the Riots*** بالتعاون بين صحيفة **الجارديان** وعدد من الجامعات البريطانية والصحفيين المستقلين والباحثين من المجتمع المحلي. جمع المشروع، والذي أسس لإعداد هذه الدراسة، نحو 2.6 مليون تغريدة حول أعمال الشغب التي وقعت في أغسطس 2011، وتوصل إلى عدد من الاستنتاجات، منها أنه كان هناك عدد قليل جداً من التغريدات التي استخدمت للتعبير عن النشاط الإجرامي أو تشجيعه. ومع ذلك، تم جمع مجموعة من التغريدات باستخدام نحو 150 وسماً "Hashtag"، ما يعني أن التغريدات المرتبطة بوسم محدد، مثل "شغب لندن# Londonriots#"، هي التي تم جمعها وتحليلها. ومع ذلك، من الممكن أن يكون الناس الذين يستخدمون وسماً عندما يغرّدون لا يمثلون جميع التغريدات المتعلقة بأعمال الشغب. فعلى سبيل المثال، ربما يقل احتمال تحدثهم عن نشاطات إجرامية لأن الوسوم عادة ما تُوظف من قبل المستخدمين لإيصال التغريدات إلى جمهور أوسع نطاقاً. في علم الإحصاء، يُعرف هذا بأنه «مفقود في بيانات غير عشوائية»؛ بمعنى أن بيانات محددة قد تفقد بشكل منهجي نتيجة أسلوب أخذ العينة. وتعد هذه مشكلة خطيرة عند الخروج باستنتاجات، لأنه عندما يغيب الناس عن مجموعة بيانات تمثيلية لسبب ما وليس مصادفة، فإنهم يتشاركون سمة (أو سمات) قد يكون لها أثر مهم على مخرجات البحث، وغالباً ما تكون تلك السمة مهمة.

وبخلاف الوضع في بحوث العلوم الاجتماعية، قد تؤثر الاعتبارات الفنية أيضاً في جودة العينة. ففي حالة تويتر، على سبيل المثال، تقتصر واجهة التطبيق المتوافرة للعامة على 150 طلباً في الساعة، ويصل هذا إلى نحو 20000 طلب عندما تدرج في "القائمة البيضاء". ومع أن هذا قد يجذب مجموعة بيانات هائلة بمقاييس العلوم الاجتماعية التقليدية، فإنه قد يجذب كمية صغيرة فقط، وليس عينة تمثيلية تلقائية، من إجمالي عدد التغريدات بالنسبة إلى تويتر. ويمكن أن يتمكن الباحثون من الوصول إلى نسب أكبر من مصادر تغذية التغريدات.

وهناك عدد من مستويات الوصول إلى بيانات تويتر، حيث يوفر مستوى Firehose الوصول إلى جميع التغريدات، في حين يوفر Gardenhose الوصول إلى 10٪، أما Spritzer فيوفر 1٪. وللأسف، فإن مدى دقة تأثير مستويات الوصول المختلفة في جودة البيانات، وأنواع التحيز المنهجي التي قد تخفيها غير معروفة بشكل كامل، ونادراً ما تذكر.

لخدمة السياسة العامة، بما في ذلك الاستراتيجيات الأمنية، يجب تطوير خطط للحصول على البيانات بحيث تسمح بالربط ما بين سلوك المستخدم عندما يكون متصلاً بالإنترنت وسلوكه عندما لا يكون متصلاً بالإنترنت. ويعد مفتاح ذلك التمثيل الديمغرافي. ذلك أن الأشخاص الذين يستخدمون وسائل التواصل الاجتماعي مثل تويتر وفيسبوك يميلون إلى أن يكونوا أصغر سناً وأكثر ثراءً وتعلماً وتحضراً مقارنة بباقي السكان بشكل عام.[25] إضافة إلى ذلك، عند النظر إلى التركيبة الديمغرافية، لا يكون السكان بشكل عام هم العامل المهم فقط، بل المجتمع الذي يمثل المعلومات التي يتم جمعها. هذا ويخضع المحتوى الاجتماعي على الإنترنت إلى التأثر الدائم بمبدأ باريتو* لما يعرف بـ"القلة الحيوية" وهو أن 80٪ من المحتوى الذي ينتجه المستخدمون في أي موقع إلكتروني يميل إلى أن يأتي من 20٪ من المستخدمين ذوي الإنتاجية العالية.[26] وقد توصلت دراسة أجريت في عام 2010 على تويتر إلى أن هذا صحيح إلى حد كبير؛ فقد وجد أن 22.5٪ من المستخدمين فقط هم الذين يشكلون نحو 90٪ من النشاطات كافة.[27]

المعالجة والتحليل

كما وصفنا في القسم السابق، يمثل استخلاص استنتاجات ذات مغزى من بيانات وسائل التواصل الاجتماعي تحديات كبيرة لمحلل الاستخبارات. وكثير من الوسائل التقانية التي تم تطويرها في القطاع الخاص بوساطة أقسام الإعلانات والعلاقات العامة قد تشكلت استناداً إلى مقاييس تلائم احتياجات تلك الصناعات؛ فهي تهدف إلى الحصول على فهم عام للآراء الخاصة بمنتج ما أو عما إذا كانت حملة إعلانية جديدة تُحدث "ضجة".

---

* نسبة إلى ولفريد فريتز باريتو، وهو عالم اقتصادي واجتماعي إيطالي (1848- 1923)، وصاحب المبدأ المعروف بقاعدة 80-20 في علم الإدارة. (المترجم)

ومع ذلك، تتطلب الجهود الأمنية والاستخبارية نماذج تحليل من تلك التي يمكن أن تقدم مستويات من الثقة التي لا يمكن أن تقدمها تلك الوسائل التقانية.

ولأن مجموعات بيانات وسائل التواصل الاجتماعي ضخمة للغاية، فقد تم تطوير عدد من الطرق الحسابية للاستدلال واستخراج "المعنى" تلقائياً، من دون وجود محلل بشري كما هو معهود. وأهم طريقة هي شكل مختلف من أشكال الذكاء الاصطناعي؛ وهو "التعلّم الآلي" Machine Learning؛ إذ يتم ضبط الخوارزميات بحيث تستطيع تمييز الأنماط، ومن ثم المعنى الموجود في أجزاء المعلومات، وبهذا لن يكون الإنسان بحاجة إلى الاطلاع عليها. ثمة عدد من التطبيقات المهمة للتعلم الآلي، تراوح بين تحديد المجموعات والانحرافات في مجموعات البيانات الضخمة واستخراج المعلومات الدلالية من النصوص. ويعد أحد التطبيقات المهمة على وجه الخصوص هو "تحليل المشاعر"؛ إذ يبحث النظام الحسابي عن صفات وسمات محددة في جزء من النص ليربطه بعاطفة أو "شعور". بمجرد أن يحدد المُدخِل الإنساني الكلمات المفتاحية التي تشير إلى المشاعر التي يجري البحث عنها، والنماذج النصية لهذه المشاعر، تستطيع الخوارزمية، بدرجات متفاوتة من التحديد والدقة، أن تصنف على هذا الأساس كميات هائلة من البيانات بطريقة آلية. وقد تم تطبيق تحليل المشاعر على عدد من الأهداف، بدءاً من قياس مشاعر مستخدمي تويتر تجاه الأحزاب السياسية إلى التنبؤ بمستقبل عوائد شباك التذاكر.[28] وفي المستقبل، ربما نشهد استخدام تحليل المشاعر من قبل الشرطة في جس نبض المتظاهرين واحتمال اندلاع أعمال عنف إجرامية.

تتيح القدرة على استخراج المعنى بشكل تلقائي من بيانات غير مهيكلة، مثل التغريدات، فرصاً بحثية كثيرة، وأصبح بإمكان الباحثين الاجتماعيين الآن التفكير في معالجة معلومات، وإعداد مجموعات عينات، على نطاق لم يكن ممكناً من قبل. ومع ذلك، من بين العواقب الحاسمة لانتشار أسلوب التعلم الآلي داخل تحليلات وسائل التواصل الاجتماعي هو أننا أصبحنا في هذا الوقت أكثر قدرة على حساب السلوك الإنساني على الإنترنت من تقديم تفسير نقدي حول أسبابه ومعانيه.

للتوصل إلى مثل هذا المغزى في أي شكل من أشكال التواصل، يـؤدي السـياق دوراً حاسماً؛ إذ إن إحدى الركائز المحورية في علم الإشارات واللغويات هـي أن اللغـة تُشـكّل وتُبنى؛ فالقصد، والدافع، والأهمية الاجتماعية، والإشارة، والدلالة لأي حديث كلها قابلة للتحول والتبدل اعتماداً على سياق الموقف والثقافة. وتعتمد دقة أي تفسير على فهم مفصّل جداً للجماعة أو السياق الذي تتم دراسته. على سبيل المثال، معظم الجماعات تستخدم لغـة محلية أو لغة خاصة بالمجموعة، ومن ثم، فإن استخدام مفـردات أو قـاموس مـن المشـاعر النمطية أو العامة سيعطي في الغالب تفسيرات خاطئة.

ومع ذلك، نظراً إلى أن معالجة الكم الهائل من البيانـات المتاحـة حاليـاً يتطلـب جمـع البيانات بطريقة آلية، فغالباً ما يتم فقْد كثير من الإشارات السياقية في تحليل بيانات وسائل التواصل الاجتماعي مثل سلسلة النقاش، والمعلومات المتعلقة بالمتحدث، ولهجة الحديث. ومن ثم، يجب استخلاص الأحاديث من الصورة الأوسع الخاصة بـالموقف أو السـياق أو الثقافة؛ أي من "سياقه الطبيعي". ذلك أن عملية "أخذ عينة" من منصة وسـائل التواصـل الاجتماعي (كجمع التغريدات أو المشاركات عـلى فيسـبوك) تشـبه الاختيـار عـن طريـق (الفلترة) في استخبارات الإشارات، فهي لا تكفي في العـادة بمفردهـا لتوضـيح وضـعية الحديث في الشبكة الاجتماعية (مثل هل كان الحديث مـع صـديق أو كـان غـير ذلـك) أو شبكة المحادثة (مثل هل كان الحديث عبارة عن دفاع حاد في جدال محتـدم). مـرة أخـرى، هذه هي قضايا واجهتها وكالات استخبارات الإشارات في عصـر الإنترنت، حيث ثبـت أن الخبرة التحليلية والتقدير السليم هما العاملان الرئيسيان.

يتشكل السياق أيضاً من خلال المعايير والأعراف المتبعـة في وسـيلة التواصـل التـي نستخدمها. بدأت دراسات عدة في تحديـد الأعـراف والقواعـد والسـلوكيات التـي تُمـلي التواصل عبر وسائل التواصل الاجتماعي على الإنترنت، والتي تختلـف بشـكل كبـير عـن الكيفية التي قد يتواصل بها الناس خارج إطار الإنترنت. إذ تشير بعـض هـذه الدراسـات على سبيل المثال إلى «التأثير التحرري للتواصل عبر الإنترنت»؛ بمعنى أن كـون الشـخص غير مرئي ومجهول الهوية بالنسبة إلى الآخرين في تواصله عبر الإنترنـت، فـإن ذلـك يقـوده لاستخدامات لغوية أكثر تحرراً وأكثر تركيزاً وإفصاحاً عن النفس وأكثـر جـرأة.[29] كـما أن

الارتباط بمجموعات أو حركات قد تغيّر أيضاً؛ فالأشكال التقليدية للعضوية لمجموعة أو حركة كبيرة نسبياً تتضمن في الغالب رسوم اشتراك وقوائم عضوية. ومع ذلك، بالنسبة إلى كثير من المجموعات عبر الإنترنت، يكفي الضغط لمرة واحدة على الفأرة للتعبير عن لون من ألوان الانتماء. وهذا الشكل من أشكال الانتماء هو الأسرع زوالاً، والأكثر مرونة، وربما الأقل تطلباً للانخراط. وفي الواقع، توصلت دراسة حديثة شملت نحو 1300 من مشجعي رابطة الدفاع الإنجليزية English Defence League على الفيسبوك إلى أن ثلاثة أرباعهم فقط يعدّون أنفسهم "أعضاء" في المجموعة، وأن ربع العدد فقط قد شارك فعلياً في مسيرة.[30]

تشكل هذه الظواهر معاً الظهور السريع لثقافات فرعية مميزة لوسائل التواصل الاجتماعي، التي تسهم في تطوير مفاهيم جديدة وأعراف اجتماعية واستخداماتٍ للّغةِ بطرائق واضحة مميزة.[31] وبالفعل، هناك حقل جديد من علم الاجتماع، وهو علم الاجتماع الرقمي، مخصص لفهم التأثيرات الاجتماعية-الثقافية للإنترنت والطرق الجديدة التي تستخدم بها.

إن عدم أخذ السياق في الاعتبار، قد يؤدي إلى حدوث تداعيات كبيرة، وقد يقود إلى سوء تفسير الحديث. في عام 2010، أعلن بول تشامبرز Paul Chambers لأتباعه الذين يبلغ عددهم 650 شخصاً على تويتر عن عزمه «نسف مطار [روبن هود]!!».[32] لاشك في أنه قال ذلك مازحاً، لكنه أُدين بشكل أولي على خلفية "استخدام نظام الاتصالات العامة في التهديد" وفقاً لقانون الاتصالات لعام 2003، وأثارت إدانته موجة انتقادات عامة واسعة، وتم إسقاط هذه الإدانة في الاستئناف. أشار القاضي المعروف جوناثان بنيت Jonathan Bennett، إلى أن «المخاوف الأمنية البالغة» تكمن في سياق الأوقات التي نعيشها، ولكن ربما ليس في سياق ثقافي وظرفي محدد من الكلام على تويتر.[33] في قضية مشابهة، تم منع كل من لي فان بريان وإيميلي ونتنج من دخول الولايات المتحدة الأمريكية عقب إرسال تغريدة على تويتر قالا فيها: «تفرغوا هذا الأسبوع لنميمة سريعة/ جهزّوا قبل أن أذهب وأدمر أمريكا؟».[34]

وعلى الرغم من أنه لا توجد هناك حلول لهذه الصعوبات، فإنـه يمكـن اتخـاذ بعـض الخطوات. أولاً، يجب أن تصبح أدوات معالجة البيانات الضخمة أكثـر "ملاءمـة للقيـاس البشـري"؛ أي أكثر ملاءمة للموضـوع الإنسـاني الـذي ثمـة رغبـة في قياسـه. ويجـب أن تتضمن الطرق الإحصائية التحليلية مثل "تحليـل المشـاعر" محللـين وخـبراء ممـن يفهمـون أعراف الجماعات وسلوكياتها محل البحث. ثانياً، يتعـين أن يعتمـد أي تحليـل لمجموعـات بيانات وسائل التواصل الاجتماعي دائماً عـلى فهـم للوسـيلة ذاتهـا: الثقافـة المحـددة عـلى الإنترنت واللغة والسلوك. وفي هذا الصدد، يعد مشـروع راينارد Project Raynard أحد البرامج الجيدة والحديثة نسـبياً التـي تشـدد عـلى أهميـة تأسـيس الأعـراف أولاً في بيئـات الإنترنت قبل البحث عن الانحرافات في الأعراف.[35] والأهم من ذلك، هو أن أي منظمـة تسـتخدم اسـتخبارات وسـائل التواصـل الاجتماعـي يجـب أن تـدرك القيـود التحليليـة والتفسيرية لهذا الحقل، وكيـف تـنعكس هـذه القيـود عـلى نوعيـة الأفكـار التـي يمكـن استخلاصها، ونوع القرارات التي يمكن التوصل إليها في ظل مثل هذه القيود.

النشـر

يعتمد الاستخدام الفعّال للمعلومات الاستخبارية المستقاة من مصادر الإنترنت بـما في ذلك مجموعـات بيانـات وسـائل التواصـل الاجتماعـي عـلى إيصـالها إلى الأشـخاص المناسبين بســرعة، وبصـورة آمنـة، وتقـديمها في شـكل يجعلهـا ذات أهميـة اسـتراتيجية وعملياتية لصناع القرار. واعتماداً على الهدف من استخبارات وسائل التواصل الاجتماعي، قد يتخذ النشــر أشـكالاً عديـدة، تـراوح مـن الأوراق التحليليـة الاسـتراتيجية المعمقـة المعتمدة على المراجع والتي تقدم تحذيرات وتوصيات، إلى الاسـتخدام العمليـاتي للشاشـة الواحدة، والبيانات المرئية التي تقدم في الزمن الحقيقي وتتوافر على الأجهزة المحمولة.[36]

هنـاك عديـد مـن التحـديات التـي تجـب معالجتهـا. أولاً، يتعـين أن يعكـس نشــر المعلومات الاستخبارية لوسـائل التواصـل الاجتماعـي الصـعوبات العامـة في اسـتخدام استخبارات هذه الوسائل، مثل تعقيـدات البيانـات، وحجمهـا، وديناميتهـا – وأخـذاً في الاعتبار المشكلات الموضحة أعلاه المتعلقة بسـبل الوصـول والتفسـير – وأي عـرض لهـا يجب أن يقدم مع إجراءات أو محاذير جديدة.

ثانياً، يجب أن يُدمج نشر المعلومات الاستخبارية لوسائل التواصل الاجتماعي في القنوات الاستخبارية القائمة مثل الشرطة وخدمات الاستجابة للطوارئ، وأجهزة المخابرات، ومركز تحليل الإرهاب، ومكتب تقييم المخاطر الوطنية التابع لمجلس الوزراء...الخ. ومع ذلك، يتطلب الأمر تدريباً محدداً للقادة على مستويات ثلاثة: ذهبية وفضية وبرونزية، وتدريباً إضافياً لضباط الصف الأول الذين قد يستفيدون من الاستخدام اليومي لمثل هذه المعلومات من الذين لا يُنظر إليهم اليوم على أنهم معنيون بشكل مباشر بالمعلومات الاستخبارية.

ثالثاً، يجب أن يخضع نشر المعلومات الاستخبارية لوسائل التواصل الاجتماعي والاحتفاظ بها لأعلى معايير أمن المعلومات وحمايتها. ويتعين تطبيق الضوابط القائمة لضمان الحفاظ على أن يتم الوصول إلى بيانات استخبارات وسائل التواصل الاجتماعي بموجب إذن رسمي، ويتم تنظيم نشرها، بما في ذلك في الخارج. ذلك أن النشر غير المنظَّم لهذه البيانات من شأنه أن يقوض ثقة الرأي العام في هذا الشكل من الاستخبارات. وبصفة عامة، سواء فقدت البيانات، أو حفظت بطريقة غير آمنة، أو تعرضت لاختراق عدائي، في ظل زيادة الحكومة لكمية المعلومات الشخصية التي تحتفظ بها، فهناك إمكانية لانكشاف هذه البيانات، وبهذا سيزداد حتماً الأذى الذي تلحقه بثقة الرأي العام فيها.

رابعاً، سيكون التطبيق الفعّال لأساليب العرض التصويري للبيانات أمراً مطلوباً بغية تحويل المعلومات الاستخبارية المعقدة والمتشابكة في كثير من الأحيان إلى شكل أكثر وضوحاً، ولكن مع الحفاظ على الطبيعة المتشابكة للمعلومات. تحتاج وكالات إنفاذ القانون على وجه التحديد إلى اكتساب مزيد من الخبرة في استخدام أساليب تحليل بيانات استخبارات وسائل التواصل الاجتماعي لكي تطور قواعد ولوائح تفصيلية لإدارتها على نحو آمن.

التحقق والصلاحية والاستخدام

ترتبط الطريقة التي يمكن أن تقدم بها استخبارات وسائل التواصل الاجتماعي قيمة مضافة بكيفية استخدام المشغلين (مثل ضباط الشرطة في خط المواجهة) فعلياً

للمعلومات، وبكيفية تفسيرها والتصرف بناء عليها (مثل نشر قوات احتياطية في مرحلة الاستعداد لانطلاق مسيرة). وبالإضافة إلى العقبات المنهجية الكثيرة التي تقف في وجه التفسير المسؤول للبيانات، فإن وسائل التواصل الاجتماعي التي تتم مراقبتها تكون عرضة لتضمّن معلومات مضلِّلة وذات طبيعة جدلية، وربما تنطوي على إعادة نشر أنصاف حقائق بصورة انتقائية، وأخطاء وتشويهات صريحة. ومن ثم، يعد التحقق من صلاحية معلومات استخبارات وسائل التواصل الاجتماعي وظيفة مهمة لمحلل هذه الوسائل.

ومن المخاطر التي يتعين التنبه عليها عند التحقق من بيانات استخبارات وسائل التواصل الاجتماعي خطر هندسة "تأثير المراقبة"؛ بمعنى ميل الأفراد لتغيير سلوكهم إذا شعروا أنهم مراقبون. في عام 2009، حذرت "شبكة الانخراط في السياسات" التابعة لكلية لندن للاقتصاد LSE's Policy Engagement Network من هذا "التأثير" في تقرير قُدمّ استجابةً لبرنامج تحديث اعتراض الاتصالات الذي سعت الحكومة البريطانية آنذاك لتبنيه. أعرب التقرير عن مخاوفه من أنه عندما يدرك الرأي العام أنه يتم جمع بيانات الاتصالات وتصنيفها، فقد يقود ذلك إلى إحداث تأثير سلبي في حق الفرد في حرية التعبير وحرية التجمع، وربما يثني الناس عن المشاركة في القيام بالاتصالات.[37]

على الجانب الآخر، ثبت أن التوقعات السابقة التي تنبأت مثلاً بتراجع المعلومات الاستخبارية المستقاة من الاتصالات نتيجة لبرامج التشفير المتوافرة، غير صحيحة. وعلى نحو مشابه، من غير المتوقع أن تؤدي التغيرات الحاصلة في سلوك الجمهور نتيجة لمعرفته بوجود مراقبة لوسائل التواصل الاجتماعي، إلى تقليص كبير في فاعلية وسائل التواصل الاجتماعي وبيانات الاتصالات عبر الإنترنت باعتبارها مصادر للاستخبارات.

تتصل بهذه القضية مشكلة "التلاعب"؛ وهو الاستخدام المتعمد لوسائل التواصل الاجتماعي بهدف تضليل المراقب أو إرباكه، أي تضليل أجهزة إنفاذ القانون. في سياق العمل الاستخباراتي، لا تعد هذه المشكلة جديدة، فالخبرة تفيد بوجودها سابقاً مثل عمليات خداع دول التحالف في الحرب العالمية الثانية، والتي توضح الحذر الذي يجب أن يتم به تخطيط عمليات الخداع لكي لا تؤدي نتائج عكسية على صاحبها. إن طبيعة

استخبارات وسائل التواصل الاجتماعي ربما تجعل محاولات الخداع أكثر ترجيحاً في ضوء وجود وسائل التواصل الاجتماعي في كل مكان واستخدامها على نطاق واسع وإضفاء طابع الديمقراطية على تشفير الحاسوب والمعرفة الفنية. من بين أمثلة الحوادث التي وقعت مؤخراً، مجموعة مُسربة من رسائل البريد الإلكتروني التي زُعم أنها تخص مستشارة لبشار الأسد، تُدعى هديل، نشرت تعليقات موالية للنظام تحت هوية مفترضة على الفيسبوك، واعتقد خطأً أنها حقيقية، ومن ثم حظيت بتغطية دولية عبر شبكة **سي إن إن**.[38]

لهذه الأسباب، يجب أن تكون هناك عملية شاملة ودقيقة (ومع ذلك سريعة على نحو كاف) لضمان إمكانية التحقق من أي عنصر من عناصر المعلومات الاستخبارية لوسائل التواصل الاجتماعي قبل أن يتم إرسالها إلى المستخدم النهائي. من الناحية المثالية، يجري التحقق من صحة المعلومات الاستخبارية لوسائل التواصل الاجتماعي في مستويات أعلى في التسلسل الهيكلي للعملية، بدءاً من مهمات الوصول إلى البيانات ومعالجتها عندما يمكن استخدام مصادر المعلومات الاستخبارية كافة، بما في ذلك مواد المصادر المفتوحة.

وكما هو الأمر بالنسبة إلى مصادر المعلومات الاستخبارية الأخرى، يتعين أن تجري عملية التحقق هذه على شكل تقارير، بحيث تصنّف بعض المعلومات الاستخبارية لوسائل التواصل الاجتماعي على أنها "سرية". ومن خلال توضيح نقاط الضعف والتحيز المحتملة في الحصول على المعلومات وتحليلها، قد نستطيع قياس مدى أهمية المعلومات التي تم جمعها ونضع محاذير للاستنتاجات التي يمكن استخلاصها.

يتعين علينا أيضاً أن نكون قادرين على ربط المعلومات الاستخبارية لوسائل التواصل الاجتماعي بغيرها من الأنواع الأخرى من الأدلة لتكوين صورة عامة، أي إجراء تقييم باستخدام "جميع المصادر". يتعين أن يتم تقييم قيمة المعلومات الاستخبارية لوسائل التواصل الاجتماعي مقارنة بالأشكال الأخرى للاستخبارات، كما تتعين دراسة الطرائق التي يمكن بها استخدام الأنواع المختلفة من المعلومات الاستخبارية إلى جانبها. إن الأمر الحاسم هنا يكمن في التطبيق الدقيق لاستخبارات وسائل التواصل الاجتماعي في ظرف محدد، وفي "قوتها" مقارنة بالأشكال الأخرى من المعلومات الاستخبارية. ما يجعل الأمر

معقداً في كليهما، هو اختلافهما وفقاً للحالة المعنية، والتي تبدأ من تحديد الاتجاهات المجتمعية على مستوى واسع، إلى سياق مكافحة الشغب أو السيطرة على الحشود.

هناك عدد من الاستراتيجيات المفيدة في تطوير عمليات التحقق من استخبارات وسائل التواصل الاجتماعي. ويمكن إجراء بحوث أكثر نضجاً من الناحية المنهجية من دون الاتصال بالإنترنت، بالتوازي مع مشروعات استخبارات وسائل التواصل الاجتماعي بهدف إتاحة الفرصة لمقارنة النتائج. على سبيل المثال، سيكون من المفيد – على وجه التحديد – إرساء قواعد بشأن كيفية تحول ظواهر الإنترنت إلى سلوك خارج دائرة الإنترنت. ويمكن أيضاً تحليل البيانات بأثر رجعي لقياس دقة استخبارات وسائل التواصل الاجتماعي وتشخيص الحالات التي تم فيها تجاوز هذه الدقة. إضافة إلى مسؤوليات التحقق المحددة الملقاة على عاتق الوكالة المنوط بها جمع المعلومات الاستخبارية، يتعين أن يكون هناك تعزيز قوي لمهارات الأفرع الحكومية كافة التي قد تشترك في هذا العمل؛ فمن المستحيل استخدام هذه الوسيلة من دون محللين وضباط شرطة وقضاة يفهمون قواعدها وأعرافها. في نهاية الأمر، لن يتسنى فهم القيمة الحقيقية لاستخبارات وسائل التواصل الاجتماعي إلا عبر استخدامها. وسوف يظهر هذا الفهم تدريجياً مع تزايد استخدام استخبارات وسائل التواصل الاجتماعي، ويجب أن نتوقع درجات متفاوتة من النجاح في السياقات المختلفة.

بصفة عامة، تنشأ المخاطر الرئيسية في استخدام المعلومات من وسائل التواصل الاجتماعي بسبب غياب التفاعل بين العلوم الإنسانية والتخصصات الإحصائية والحاسوبية. ذلك أن التخصصات القادرة على فهم السلوك البشري وشرحه (أي العلوم الاجتماعية والسلوكية، وعلم السياسة، ودراسة الانتخابات السياسية، والأنثروبولوجيا وعلم النفس الاجتماعي) لم تواكب الأفكار الخاصة بالأساليب التي تتبعها تقنيات البيانات الضخمة الضرورية لفهم وسائل التواصل الاجتماعي. وعلى العكس من ذلك، يلاحظ أن أساليب البيانات الضخمة ذاتها، التي تشكل العمود الفقري للقدرات الحالية لاستخبارات وسائل التواصل الاجتماعي، لم تستخدم علم الاجتماع لتوظيف القياسات والإحصاءات التي تستخدمها لمهمة تفسير السلوك البشري على نحو ذي مغزى.

إجمالاً، تشير الخطوات المنهجية إلى تطور جوهري في القدرات المتوافرة لاستغلال وسائل التواصل الاجتماعي. ولكي تصبح استخبارات وسائل التواصل الاجتماعي قوية بما يكفي بحيث يتم اتخاذ قرارات وتغيير سياسات بناء عليها، يجب أن تعتمد على نظام أكاديمي تطبيقي جديد؛ وهو علم وسائل التواصل الاجتماعي. من شأن هذا أن يجسد انصهاراً أكبر مغزى وأكثر تكثيفاً للمناهج الحاسوبية والتقانية والإنسانية. وتعد الطريقة الوحيدة لكي تصبح تفسيرات سلوك البشر التي تتم اعتماداً على البيانات، تفسيرات ذات طبيعة بشرية أيضاً، هي إحداث إدماج بين تلك التخصصات. ويقتضي ذلك بناء علاقات جديدة مع عالم الصناعة والأوساط الأكاديمية، مترافقة مع استثمارات منسقة وطويلة الأجل، وذلك لبناء قدرات تقانية ومنهجية، وللتمكن من عرض هذا الحقل الجديد بجدارة.

الشرعية

يعدّ الشرط الثاني المهم لاستخدام استخبارات وسائل التواصل الاجتماعي هو أن تعمل هذه الاستخبارات بصورة شرعية. بشكل عام، ترتكز النشاطات الأمنية والاستخباراتية كافة على تحقيق توازن دقيق بين ثلاث فئات من المصالح العامة: الحفاظ على الأمن القومي بما في ذلك النظام العام والسلامة العامة، وحق المواطنين في سيادة القانون والحرية والخصوصية، والرفاهة الاقتصادية والاجتماعية الشاملة للبلاد ومواطنيها. ولكي يكون استخدام استخبارات وسائل التواصل الاجتماعي شرعياً، يجب أن يأخذ في اعتباره المخاطر التي تسبب ضرراً للمصلحة العامة، وأن يوازن هذا مع أي مساهمة يقدمها.

في معظم الحالات، يتعين أن تعزز هذه الفئات الثلاث من المصالح العامة بعضها تجاه بعض: الأمن يعزز الاستثمار في الداخل، وثقة السوق تعزز الرفاهة الاقتصادية والوئام الاجتماعي، الذي يدعم بدوره الحفاظ على الأمن. ومع ذلك، ثمة أوقات يجب أن يتم فيها الاختيار؛ إذ يكون المبرر الوحيد لتعريض مصلحة عامة للخطر هو توفير مصلحة أخرى، على أن يتم ذلك كله في إطار نهج قائم على أساس الحقوق. ومع ذلك، تعد وسائل التواصل الاجتماعي ذات احتمالات تخريبية أيضاً؛ إذ أحدثت تأثيراً بالفعل، وفي بعض

الحالات تعيد تحديد الكيفية التي يمكن بها تحقيق الفئـات الـثلاث مـن المصـالح العامـة، وذلك للأسباب التالية:

- التماثل والتغاير: تخترق استخبارات وسائل التواصل الاجتماعي عدة فئات، ويمكـن أن تمثل أكثر من فئة في وقت واحد؛ ففحص التغريدات على نطـاق واسـع لـه أوجـه تشابه مع المراقبة الجماعية مثل نشـر كاميرات المراقبـة التلفزيونيـة في أمكنـة مزدحمـة. وتتشابه المتابعة الحثيثة لصفحة شخص ما عـلى الفيسـبوك خـلال مسـار تحقيـق مـع المراقبة البصـرية التي "يمكن أن يسمح بها" ضـابط شـــرطة رفيـع المسـتوى. كـما أن الوصول إلى رسائل البلاكبيري المشفرة عن طريق كسـر الرقم السـري هـو اعـتراض للاتصالات بموجب قانون تنظيم صلاحيات التحري لسنة 2000 RIPA في المملكة المتحدة، ويتعين الحصول على إذن لتنفيذه.

- العموميـة: عنـدما تسـتخدم اسـتخبارات وسـائل التواصـل الاجتماعـي لأغـراض التحقيق الفضولي ربما لا يكون هناك اسم يُشتبه فيه أو رقم هاتف يتم استهدافه، وربما تكون النتيجة عامة وليست محددة لفرد بعينه (مثل ملاحظة زيادة في الاتصالات عـبر وسائل التواصل الاجتماعي في منطقة بعينها حيث تندلع المظاهرات).

- قابلية التوسع: تمكن زيادة قدرة عدة أساليب آلية لجمع البيانات، لتزيـد قـدرتها مـن جمع المئات إلى جمع الملايين من أجزاء بيانـات وسـائل التواصـل الاجتماعـي بسـهولة وبأسعار زهيدة. وقد يكون من الصعب تحديد الحجم مسبقاً.

- المرونة: يمكن تغيير مضمون عديد من تقنيات "فحص" وسائل التواصل الاجتماعي (مثل الكلمات المفتاحية التي يتم البحث عنها) بسهولة. وهذا يعني أنه يمكن بسهولة إعادة توجيهها بعيداً عن مهمتها ووظيفتها الأصلية، التـي ربـما يمكـن تبريرهـا مـن الناحية العملياتية بتغييرات تكتيكية على الأرض.

- غير مرئية: مثل غيرها من أشكال المراقبـة السـرية الأخـرى، لـن تكـون العمليـة في العادة مرئية بالنسبة إلى مستخدمي وسـائل التواصـل الاجتماعـي أنفسـهم، وسـوف تتغلب على ما قد يفترضون أنها إعدادات لحفظ الخصوصية.

- مخاوف شعبية أوسع بشأن المراقبة الرقمية: يجب أن يتم فهم استخبارات وسائل التواصل الاجتماعي في إطار المخاوف الشعبية بشأن المراقبة الرقمية نتيجة للزيادة الكبيرة في نظُم المعلومات التي لديها قدرات هائلة على جمع المعلومات وتخزينها واستعادتها وتوزيعها وعرضها ونشرها. تنشأ المخاوف من زيادة فرص المراقبة في البيئة الغنية بالبيانات، وعواقب التسلل العرضي، وإمكانية انكشاف البيانات، والأثر العام للاشتباه بارتكاب الجرائم نتيجة لجمع المعلومات على نطاق واسع.[39]

وكما هي الحال مع الأشكال الأخرى للاستخبارات، تجب معالجة المخاوف العامة المتعلقة بالخصوصية. وتجدر الإشارة هنا إلى أن الخصوصية نفسها مفهوم محير؛ إذ تكرس المادة 8 من "الاتفاقية الأوروبية لحقوق الإنسان" الحق في احترام «حياة الشخص الخاصة والعائلية ومنزله ومراسلاته». قد يعني احترام الخصوصية ضرورة الحفاظ على سرية البيانات، وجمعها من دون تحديد الهوية، واستخدامها حسبما يقرر الشخص (وفق مبدأ الموافقة المسبقة)، وأن يكون الناس قادرين على رؤيتها وتصحيح الأخطاء، أو ألا يتم جمع بيانات على الإطلاق، بالطبع.

ومع ذلك، يسهم عديد من التغييرات الواسعة والأساسية في المجتمع في تحويل ماهية معنى الخصوصية بالنسبة إلى الناس. ويشكل استخدام وسائل التواصل الاجتماعي بشكل خاص تحدياً للفروق الواضحة بين ما هو خاص وما هو ليس كذلك. وتشير إحصاءات معهد ماكينزي العالمي إلى أنه تتم مشاركة 30 مليار جزء من المحتوى على الفيسبوك كل شهر، وكثير منها بيانات شخصية.[40] إن مشاركة كمية كبيرة لمثل هذه البيانات الشخصية التي يتم تحميلها طوعاً، وكذلك العدد الكبير من الأفراد والمؤسسات الذين يمكنهم الوصول إلى هذه البيانات، لم يسبق له مثيل. واعتماداً على إعدادات الخصوصية التي يتم ضبطها وفق اختيارات المستخدم، فإن المعلومات الشخصية التي تتم إضافتها إلى الفيسبوك يمكن أن يستعرضها جميع مستخدمي الفيسبوك الآخرين الذين يبلغ عددهم نحو 845 مليون مستخدم. يعد هذا الانتشار الواسع النطاق للمعلومات الشخصية أمراً جوهرياً لرواج مواقع الشبكات الاجتماعية. يُشار إلى أن إعدادات الخصوصية في موقع الفيسبوك تُعلِم المستخدمين بأن القدرة على مشاركة المعلومات «تتيح لنا تقديم الفيسبوك

بالصورة التي هو عليها اليوم»، في حين يذكر موقع تويتر بمزيد من الصراحة أن «معظم المعلومات التي تقدمها لنا هي معلومات تطلب منا أن نجعلها عامة».[41] ونتيجة لهذه السلوكيات المتغيرة، أعلن مارك زوكيربيرج Mark Zuckerberg، الرئيس التنفيذي لفيسبوك، أن الخصوصية «لم تعد قاعدة اجتماعية».[42] معظمنا يقبل بأن تقوم كل من المؤسسات الخاصة والعامة (مثل تيسكو Tesco وكلبكاردز Clubcards وأمازون Amazon وأويستر Oyster وجوجل) بمعرفة كمية هائلة من البيانات الخاصة بنا وتسجيلها يومياً. في استطلاع أجرته مؤسسة "يوروباروميتر" Eurobarometer، اعتبرت أغلبية ضئيلة من الذين جرى استطلاع رأيهم في المملكة المتحدة أن صورهم تُعد بيانات شخصية، في حين اعتبرت نسبة أقل من النصف أن "أصدقاء الشخص" هم من ضمن البيانات الشخصية، وترى نسبة 41٪ أن تفاصيل المواقع التي يزورونها هي بيانات شخصية، و32٪ ترى أن أذواقها وآراءها هي بيانات شخصية. في مقابل ذلك، ترى أغلبية كبيرة أن البيانات المالية هي بيانات شخصية.[43] ومع ذلك، وعلى رغم أن الأبحاث تشير إلى أن المستخدمين يدركون أن كشف المعلومات الشخصية هو جزء متنامي الأهمية في الحياة الحديثة، فإن لدى أغلبية المستخدمين مخاوف بشأن معنى هذا.[44] وفي استطلاع للرأي أجرته المفوضية الأوروبية في عام 2008، قال ما نسبتهم نحو 80٪ من الذين جرى استطلاع رأيهم إن وعي "الناس" بحماية البيانات الشخصية في المملكة المتحدة ضعيف.[45]

ويصعب قياس المواقف بشأن الخصوصية بموضوعية، ولاسيما المواقف الشائعة والعامة التي تستند إلى مبادئ. تشير القواعد السلوكية المنتشرة، مثل حجم المعلومات التي نتشاركها الآن، إلى أن المفهوم في حالة سيولة، ويُعاد على نحو جذري رسم حدود التعريف. وسوف يتواصل الجدل بشأن أين توجد الآن هذه الحدود التي أعيد رسمها بشأن امتلاك المعلومات الشخصية ومشاركتها واستخدامها، بل في الواقع ما هي الخصوصية؟[46]

تكمن المشكلة الأساسية لاستخدام الحكومة أنواعاً مختلفة من استخبارات التواصل الاجتماعي في أن الإطار المستخدم في معرفة انتهاكات الخصوصية ومعالجتها يواجه صعوبة في مواكبة العادات والمواقف الاجتماعية المتغيرة. هناك عديد من الأساليب التي يمكن أن تستخدمها الدولة في جمع المعلومات المتعلقة بالناس والاستفادة منها، وتوجد

نظُم مختلفة للقيام بهذا. كل نظام يعرف ويحدد الضرر المحتمل الذي قد يترتب جرّاء الحصول على معلومات شخصية. فعلى سبيل المثال، عندما تقوم الدولة بإجراء بحث سريري، يتم أخذ الموافقة أولاً، وعادة ما يتم ضمان عدم كشف الهوية، وعندما تستفيد الدولة من الأبحاث التي قام بها آخرون، يتم تطبيق الاستخدام العادل وينسب الفضل للأفراد المعنيين. وعندما تحصل الدولة على معلومات لتحديد الهوية مثل عينة من الحمض النووي لشخص مشتبه فيه، لا يتطلب الأمر الحصول على موافقته، ولكن يتم تطبيق قيود على الاحتفاظ بمادة العينة. وعندما تقوم الدولة بعملية المراقبة، يكون النشاط في العادة سرياً ويكون الحصول على موافقة الفرد أمراً غير مناسب. ومن ثم، فإنه للتصدي للمخاوف المتعلقة بالخصوصية واختراقها، يجب أن تكون هناك موافقة من المجتمع، يتم التعبير عنها من خلال تشريعات تفويضية؛ أي تخول الأجهزة المعنية بذلك. ومع أن التشريعات التفويضية تختلف من دولة إلى أخرى، إلا أنها قائمة على العلاقة بين مستوى الضرر من ناحية، وسلسلة الخطوات التي تُتخذ لتخفيف الضرر من ناحية أخرى (بما في ذلك طرائق الحصول على إذن والمساءلة والضرورة). وبما أن مفهوم الخصوصية أصبح الآن قابلاً للتغيير بهذه الطريقة، فمن الصعب حساب هذا النوع من الضرر الأخلاقي.

الرفاهة الاقتصادية والاجتماعية

يقدم الإنترنت، بوصفه فضاء حراً ومفتوحاً وفي إطار الحدود المعقولة، فوائدَ اقتصادية واجتماعية هائلة. كما أن النشاط الحكومي يهدف إلى حماية الازدهار وليس تقويضه. وقد أشار وليام هيج، وزير الخارجية البريطاني، في عام 2011 إلى أنه «لن يكون هناك شيء أكثر فتكاً أو تدميراً من السيطرة القوية للدولة على الإنترنت التي تزدهر فقط بفضل موهبة الأفراد والصناعة في إطار سوق منفتحة على الأفكار والابتكار».[47] من ناحية أخرى، يتعين إدراك أن عملية الجمع والتحليل غير المنظم على نطاق واسع لبيانات وسائل التواصل الاجتماعي من قبل الشركات والحكومات على السواء (حتى ولو كان مصدراً مفتوحاً) تنطوي على خطر تقويض الثقة في هذا الفضاء وفي قيمته. ولا تعد جديدة الفكرة القائلة بأن الفوائد الاقتصادية والاجتماعية للإنترنت قائمة على افتراض انفتاحه وانعدام الرقابة الحكومية عليه. فمن مطلع التسعينيات ثمة حجة ورؤية قوية بشأن فائدة الإنترنت

والصورة التي تنبغي أن تكون عليها؛ فهي فرصة للتطور والتحول من نظام الدولة القومية إلى مجتمعات ما بعد الحدود الإقليمية، التي تتمتع بحكم ذاتي، والتي تعمل بموجب عقودها الاجتماعية غير الثابتة القائمة على الموافقة من خلال الاستخدام. وقد قال جون بيري بارلو في إعلانه الشهير عن استقلال الفضاء الإلكتروني لحكومات الدول الصناعية إن الفضاء الإلكتروني يطور سيادته بنفسه و«أنتم غير مرحب بكم بيننا».[48]

نعتقد أنه من المهم التفريق، مثلما سعينا في هذه الدراسة، بين المصدر المفتوح؛ أي استخبارات وسائل التواصل الاجتماعي غير الاختراقية (التي لا تراقب أو تخترق معلومات المستخدمين)، وبين المصدر المغلق؛ أي استخبارات وسائل التواصل الاجتماعي الاختراقية (المعنية بالمراقبة وتحديد هوية المستخدم). ومن ثم، فإن أي إطار يتمتع بالشرعية ويُمكّن من جمع استخبارات وسائل التواصل الاجتماعي واستخدامها، يجب أن يبدأ بالتفريق بين الإجراء الذي يُعد مراقبة اختراقية وما هو ليس كذلك. وهذا بدوره يجعلنا ندرك أن هناك أوقاتاً يمكننا فيها السعي بشكل شرعي للرقابة على أي معلومات نقدمها وكيفية استخدامها، ولكن هناك أوقاتاً أيضاً يجب فيها تجاوز سيطرة الأفراد. وتعتمد الظروف التي يمكن أن يحدث فيها هذا على القرارات والموافقة الجماعية بشأن سلطة الدولة.

يعد المفهوم الرئيسي المناسب لهذا التفريق هو إن كان المستخدم يتحكم في استخدام بياناته من خلال الموافقة. ولكي تكون استخبارات وسائل التواصل الاجتماعي غير اختراقية ومفتوحة المصدر، ينبغي ألا تكون لها القدرة على تحديد الأفراد، أو تُستخدم أداةً للتحقيق الجنائي، أو تخترق رغبات الخصوصية للمستخدم.

ينبغي أن يتم التعامل مع أي استخدام حكومي لاستخبارات التواصل الاجتماعي المفتوحة بالشروط ذاتها التي تخضع لها الشركات الخاصة والأوساط الأكاديمية فيما يتعلق باستخدام وسائل التواصل الاجتماعي، مع شروط تتعلق بعدم طلب ذكر الاسم وحماية البيانات. بالنسبة إلى استخبارات التواصل الاجتماعي المفتوحة، لا يُنظر إلى الضرر على أنه انتهاك للمجال الخاص لشخص ما، ولا القضايا الكبرى المتعلقة بالثقة والشك الضمني (بما أنه لا شيء من هذا سوف يحدث في إطار استخبارات التواصل الاجتماعي المفتوحة)، بل

بفقدان السيطرة على المعلومات من خلال تجاوز الاستخدام المتوقع على نحو معقول. يمكن أن تكون التوقعات المعقولة محمية من خلال سمة الانفتاح على كيفية إجراء هذا النوع من الاستخبارات أو توقيته. وينبغي أن يتم تبرير كل هذه السياسات الخاصة بجمع المعلومات والاحتفاظ بها ومشاركتها وكذلك الإعلان عن السبب في جمعها.

تعد استخبارات وسائل التواصل الاجتماعي الاختراقية هي الأكثر وضوحاً؛ إذ إن معظم الدول لديها بالفعل إطار تشريعي لتنظيم جمع المعلومات الاستخباراتية الاختراقية، لأغراض الأمن القومي مثلاً، والوقاية من الجريمة وكشفها (في حالة المملكة المتحدة تم توفير هذه السلطة في قانون عام 2000 المتعلق بتنظيم سلطات التحقيق). يمكن تقنين تطبيق مثل هذا التشريع لاستخبارات وسائل التواصل الاجتماعي الاختراقية بحيث يغطي: الصلاحيات المطلوبة للحصول على المعلومات، والإجراءات التي يجب اتباعها على المستويين القانوني والعملياتي. ومن المهم أن يكون هناك قبول شعبي للترتيبات استناداً إلى أن الرقابة المستمرة والفعالة التي تجريها الدولة قائمة على مبادئ أخلاقية سليمة. ونقترح في هذا الصدد تكييف مجموعة المبادئ التي طرحها السير ديفيد أوماند لمجتمع الاستخبارات في كتابه المعنون **تأمين الدولة**:[49]

- **المبدأ 1**: يجب أن تكون هناك قضية كافية ومستدامة. يؤكد هذا المبدأ الأول والشامل ضرورة أن تؤخذ الصورة الكبرى في الاعتبار عند القيام بأي عمل؛ مثل الأهداف العامة التي قد تبرر امتلاك جهة عامة لقدرات جمع بيانات وسائل التواصل الاجتماعي وفهمها واستخدامها. هناك خطر من أن سلسلة من إجراءات استخبارات وسائل التواصل الاجتماعي (كل بحد ذاتها يمكن تبريرها) تزحف معاً إلى نقطة نهاية غير مرغوب فيها: مستوى من المراقبة العامة غير مقبول شعبياً، وامتلاك قدرة خطيرة، والضرر الشامل لوسيلة تتمتع بقيمة جوهرية واضحة تتعدى الأمن. ذلك أن كون الشيء يمكن القيام به لا يعني أنه ينبغي القيام به. ومن ثم، فإن تطبيق مبدأ اشتراط وجود قضية كافية ومستدامة أمر ضروري من أجل: ضمان بقاء استخبارات وسائل التواصل الاجتماعي داخل الحدود المطلوبة، وتقديم فوائد اجتماعية واقتصادية وأمنية وأخرى في مجال إنفاذ القانون، ومقاومة بناء إمبراطورية

بيروقراطية، والبحث عن سبل لتوظيف الطاقات الاحتياطية أو العمل على تبسيط التقانة المتاحة من الموردين التجاريين.

- **المبدأ 2**: يجب توافر سلامة الدافع. يشير هذا المبدأ إلى أهمية سلامة الدافع في نظام الاستخبارات كله، بدءاً من بيان مبرر عملية الدخول والحصول على المعلومات نفسها، إلى التحليل الموضوعي، والتقييم والعرض الصادق للنتائج. تبرير السعي للحصول على استخبارات وسائل التواصل الاجتماعي في حالات الأفراد يجب أن يكون واضحاً على وجه الخصوص، وألا يخفي دوافع أخرى من جانب الضباط المنوط بهم إجراء التحقيق. ذلك أن المعلومات الاستخبارية بطبيعتها عادة ما تكون ناقصة وجزئية، ويمكن أن تكون خاطئة أو عرضة للخداع. وعند عرض المعلومات الاستخبارية على المستخدمين النهائيين، يجب توضيح المحددات والمحاذير بجلاء. ويجب ألا يتأثر قرار استخدام (أو عدم استخدام) المعلومات الاستخبارية، أو النتائج المستخلصة منها، باعتبارات محلية أو وطنية أو ضغط إعلامي.

- **المبدأ 3**: يجب أن تكون الأساليب المستخدمة متناسبة وضرورية. هناك مبدأ راسخ في تنفيذ القانون ينص على أن يكون حجم الضرر المحتمل الذي ينشأ عن أي إجراء يُتخذ متناسباً مع الضرر الذي يسعى لمنعه. وعند تقييم التناسب، يجب تقييم حجم التدخل. وهذا يعني حداً أدنى من المراقبة السرية للمواد التي لم يضع المستخدم قيوداً عليها، بخلاف الحالات الأخرى التي يكون لدى المستخدمين قائمة محدودة من الأصدقاء الذين يمكنهم الوصول إلى المعلومات، أو إذا كانوا يستخدمون نظاماً مثل البلاكبيري الذي يتطلب رمزاً سرياً.

- **المبدأ 4**: يجب أن يكون هناك تفويض مناسب، مصادق عليه من قبل الرقابة الخارجية. هناك مبدأ عام ينص على أنه يتعين أن توجد عملية تدقيق لإعطاء التخويل لتنفيذ إجراءات قد تتضمن خطراً أخلاقياً، على أن تكون هناك سلطة تمكن مساءلتها على نحو لا لبس فيه ضمن سلسلة قيادة واضحة. ويعد وجود مستندات كافية (أو ما يعادلها إلكترونياً) للقرارات الرئيسية أمراً حيوياً يعطي الثقة للموظفين والسياسيين ولعملية التحقيقات، ومن أجل تحقيق الإنصاف في أي حالات يشتبه في إساءة

استخدام الصلاحيات فيها. نعتقد أنه ينبغي تطبيق هذا المبدأ على استخبارات وسائل التواصل الاجتماعي، وكذلك على أي عملية استخبارات أخرى. هذه وسيلة مهمة يمكن من خلالها تحقيق التناسب والمساءلة في الممارسة العملية.

- **المبدأ 5**: يجب أن يكون اللجوء إلى الاستخبارات السرية هو الملاذ الأخير فقط، مادام استخدام مزيد من المصادر المفتوحة ممكناً. نظراً للمخاطر الأخلاقية التي تنطوي عليها أساليب جمع المعلومات الاستخبارية السرية عبر اختراق البيانات، يتعين على من يعطون إذناً بتنفيذ مثل هذه العمليات أن يسألوا إن كان يمكن الحصول على المعلومات من خلال وسائل أخرى، تراوح ما بين المصادر المفتوحة كلياً إلى المعلومات التي يتم تقديمها طوعاً وبحرية من داخل المجتمع. ولتطبيق هذا المبدأ العام على استخبارات وسائل التواصل الاجتماعي، ينبغي تفضيل الوسائل الأقل اختراقية على تلك الوسائل السرية ذات الاختراق العالي للبيانات. أما المسار الأكثر تفضيلاً فهو الوصول إلى المعلومات "الموافق عليها" صراحة من قبل مجتمع الإنترنت، مثل جمع المعلومات من المصادر الكثيرة التي تعرض طوعاً وصراحة على صفحة الفيسبوك أو "الهاشتاج". يجب أن يقتصر اللجوء إلى جمع الاستخبارات السرية (بما في ذلك عبر استغلال وسائل التواصل الاجتماعي) على الحالات التي تكون فيها المعلومات ضرورية لتحقيق غرض مشروع لعملية ما، ولا يتوقع الحصول عليها على نحو معقول عبر وسائل أخرى.

إجمالاً، تحافظ هذه المبادئ على سلسلة من الارتباطات الحاسمة؛ فمع ازدياد درجة الاختراق الذي يرافق عملية المراقبة، تزداد أهمية تطبيق ثلاثة شروط حيوية: تحديد الوكالات التي يمكن أن تقوم بتنفيذها، ومن الذي يجب أن يعطي الإذن لتنفيذها، والأسباب التي تبرر تنفيذ المراقبة بشكل شرعي. هذا أمر حيوي لتحقيق توازن بين الفائدة الممكنة من جمع المعلومات واستخدامها وبين الضرر المحتمل. ومع ذلك، فإن قياس الاختراق ليس أمراً بسيطاً؛ فغالباً ما يتشارك الناس ما قد يعتبرونها أموراً خاصة بشأن حياتهم من خلال أساليب علنية، يصاحبها أحياناً عواقب غير متوقعة أو غير مدركة. وهناك تباين كبير في حجم الاختراق الذي ينشأ عن عمليات وصول استخبارات

وسائل التواصل الاجتماعي إلى المعلومات. على سبيل المثال، تشبه عملية جمع التغريدات العلنية لشخص مشتبه فيه وتحليلها، عملية مراقبة شخص في الأمكنة العامة، أما جمع رسائل الفيسبوك لشخص ما وتحليلها، فتبدو أقرب إلى قراءة مراسلاته اليومية. ليس لدينا حتى الآن إطار مفاهيمي لما ينبغي أن يشكل خصوصية في استخدام وسائل التواصل الاجتماعي في المستقبل وأنواع الضرر المصاحبة لاختراق الخصوصية.

ملاحظات ختامية

تقدم الثورة في استخدام وسائل التواصل الاجتماعي على نطاق واسع فرصاً هائلة. لذلك يتعين على استخبارات وسائل التواصل الاجتماعي أن تصبح عضواً كاملاً في مجتمع الاستخبارات ووكالات إنفاذ القانون. ويكمن في صلب هذه العملية شرطان لا يفترقان هما: الضرورة والشرعية.

للوفاء بشرط الضرورة، يجب تطوير نظام أكاديمي تطبيقي جديد هو علم وسائل التواصل الاجتماعي. ويتطلب ذلك بناء علاقات جديدة مع عالم الصناعة والأوساط الأكاديمية، واستثمارات منسقة وطويلة الأجل لبناء قدرات على المستويين التقاني والمنهجي، وللتمكن من عرض هذا الحقل الجديد بجدارة. يجب مزج التخصصات الأفضل قدرة على فهم السلوك البشري وتفسيره (العلوم الاجتماعية والسلوكية والعلوم السياسية ودراسة الانتخابات والأنثروبولوجيا وعلم النفس الاجتماعي)، مع مناهج البيانات الضخمة اللازمة لفهم وسائل التواصل الاجتماعي. وتعد الطريقة الوحيدة لكي تصبح تفسيرات سلوك البشر المعتمدة على البيانات، تفسيرات ذات طبيعة بشرية أيضاً، هي من خلال هذا المزج بين تلك التخصصات.

ولكن التقانة والقدرة لا يمثلان سوى نصف الصورة؛ فمن أجل الوفاء بشرط الشرعية، يتعين أن يفهم الجمهور ويقبل على نطاق واسع: لماذا ومتى ووفق أي قيود يجري تنفيذ عمليات استخبارات وسائل التواصل الاجتماعي؟ ويتعين على أي حكومة ترغب في القيام باستخبارات وسائل التواصل الاجتماعي أن تتبنى نهجاً معلناً يقوم على أساس احترام حقوق الإنسان والمبادئ المرتبطة به كالمساءلة والتناسب والضرورة.

الهوامش

1. انظر:

Her Majesty's Inspectorate of the Constabulary (HMIC), *The Rules of Engagement: A Review of the August 2011 Disorders* (London: Crown Copyright 2011), especially pp. 36–9.

2. Ibid., p. 31.

3. Ibid., p. 30.

4. Ibid.

5. انظر:

'Facebook Crimes Probed by Humberside Police', *Hull Daily Mail*, 24 August 2011, <www.thisishullandeastriding.co.uk/Facebook-crimes-probed-Humberside-Police/story-13191231-detail/story.html> (accessed 17 April 2012).

وانظر أيضاً:

Westminster City Council's 'Your Choice' programme: *Choose Life, Not Gangs: Problem Kids Told to Clean Up or Face the Consequence* (City of Westminster, 29 September 2011), <www.westminster.gov.uk/pressreleases/2011-09/choose-life-not-gangs-problem-kids-told-to/> (accessed 17 April 2012).

6. انظر:

Ministry of Defence and Centre for Defence Enterprise, *Cyber and Influence Science and Technology Centre, CDE Call for Research Proposals*, 1 November 2011, <www.science.mod.uk/controls/getpdf.pdf?603> (accessed 17 April 2012).

7. انظر:

'The Value of Friendship', *Economist*, 4 February 2012, <http://www.economist.com/node/21546020> (accessed 17 April 2011).

8. انظر:

Twitterblog, *200 Million Tweets a Day*, 30 June 2011, <http://blog.twitter.com/2011/06/200-million-tweets-per-day.html> (accessed 17 April 2012).

9. انظر:

YouTube, *Statistics*, <www.youtube.com/t/press_statistics> (accessed 17 April 2012).

10. انظر:

A. Signorini, A.M. Segre and P.M. Polgreen, 'The Use of Twitter to Track Levels of Disease Activity and Public Concern in the US During the Influenza A H1N1 Pandemic', *PLoS ONE 6/5* (2011) pp.1–10.

11. انظر:

J. Hoffman, 'Trying to Find a Cry of Desperation Amid the Facebook Drama', *New York Times*, 23 February 2012, <www.nytimes.com/2012/02/24/us/facebook-posts-can-offer- clues-of-depression.html?_r3> (accessed 17 April 2012); 'T.J. Lane Facebook Photos: Suspect Faces Charges in Chardon High School Shooting (Slideshow)', *Huffington Post*, 28 February 2012, <www.huffingtonpost.com/2012/02/28/tj-lane-facebook-photos_n_1307836. html#s736080&titleTJ_Lane_Facebook> (accessed 17 April 2012).

12. انظر على سبيل المثال:

UN Global Pulse Programme, *UN Unveils Initial Findings on Uses of Real-time Data for Development Work* (UN News Centre, 8 December 2011), <www.un.org/apps/news/story.asp?NewsID40667&Crglobal&Cr1pulse> (accessed 17 April 2012).

13. انظر:

Criminal Justice Degrees Guide, *20 Infamous Crimes Committed and Solved on Facebook*, <http://mashable.com/2012/03/01/facebook-crimes/> (accessed 1 July 2012).

14. انظر:

Diego Laje, '#Pirate? Tracking Modern Buccaneers Through Twitter', *CNN*, 15 March 2012, <http://edition.cnn.com/2012/03/15/business/somalia-piracy-twitter/index.html> (accessed 1 June 2012).

15. انظر:

Jack Doyle, 'A Facebook Crime Every 40 Minutes', *Daily Mail*, 4 June 2012, <http://www.dailymail.co.uk/news/article-2154624/A-Facebook-crime-40-minutes-12-300-cases-linked- site.html> (accessed 1 June 2012).

16. انظر:

T.O. Sprenger and I.M. Welpe, *Tweets and Trades: The Information Content of Stock Microblogs*, 1 November 2010, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id =1702854> (accessed 17 April 2012).

17. انظر:

Twitter was used by pupils as an ad hoc emergency broadcasting system during the Ohio school shooting. See L. Dugan, 'Twitter Used as an Impromptu Broadcast System During Ohio School Shooting', *Media Bistro*, 28 February 2012, <www.mediabistro.

com/alltwitter/twitter-used-as-impromptu-emergency-broadcast-system-during-ohio-school-shooting_b19030> (accessed 1 June 2012).

18. .HMIC, *The Rules of Engagement*, p. 31.

19. انظر:

Howe, 'The Rise of Crowdsourcing', *Wired*, June 2006, <www.wired.com/wired/archive/14.06/crowds.html> (accessed 17 April 2012).

20. انظر:

'Reading the Riots: Investigating England's Summer of Disorder' [interactive], *Guardian*, <www.guardian.co.uk/uk/interactive/2011/aug/24/riots-twitter-traffic-interactive> (accessed 17 April 2012).

21. انظر:

Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London: HMSO 2010) p.5.

22. انظر:

R. Proctor, F. Vis and A. Voss, 'Riot Rumours: How Misinformation Spread on Twitter During a Time of Crisis', *Guardian*, 7 December 2011, <www.guardian.co.uk/uk/interactive/2011/dec/07/london-riots-twitter> (accessed 17 April 2012).

23. انظر على سبيل المثال:

J. Leskovec, J. Kleinberg and C. Faloutsos, 'Graph Evolution: Densification and Shrinking Diameters', *ACM Transactions on Knowledge Discovery from Data 1/1* (2007) <www.cs.cmu.edu/*jure/pubs/powergrowth-tkdd.pdf> (accessed 16 April 2012); J. Leskovec and C. Faloutsos, 'Sampling from Large Graphs' in T. Ellassi-Rad (chair), *Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2006* (Philadelphia: KDD 2006), <www.stat.cmu.edu/*fienberg/Stat36- 835/Leskovec-sampling-kdd06.pdf> (accessed 16 April 2012).

24. انظر على سبيل المثال:

B. O'Connor, R. Balasubramanyan, B.R. Routledge and N.A. Smith, 'From Tweets to Polls: Linking Text Sentiment to Public Opinion Time Series', *Proceedings of the AAAI Conference on Weblogs and Social Media* (Washington, DC: AIII Press 2010).

وقد جمع المؤلفون العينات باستخدام البحث من كلمات قليلة.

25. لمزيد من المعلومات حول التركيبة السكانية لتويتر وفيسبوك، انظر:

'Infographic: Facebook vs. Twitter Demographics', *Digital Buzz Blog*, 21 December 2010, <www.digitalbuzzblog.com/ infographic-facebook-vs-twitter-demographics-2010-2011/> (accessed 16 April 2012).

26. انظر:

C. Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (New York: Penguin 2008).

27. انظر:

'Twitter Statistics for 2010', *Sysomos*, December 2010, <www.sysomos.com/ insidetwitter/twitter-stats-2010/> (accessed 16 April 2012).

28. انظر:

J. Weng, Y. Yao, E. Leonardi and F. Lee, 'Event Detection in Twitter', *HP Laboratories*, 6 July 2011, <www.hpl.hp.com/techreports/2011/HPL-2011-98.html> (accessed 17 April 2012); S. Asur and B.A. Huberman, 'Predicting the Future With Social Media', *HP Laboratories*, 29 March 2010, <www.hpl.hp.com/ research/scl/papers/socialmedia/socialme-dia.pdf> (accessed 17 April 2012).

29. انظر:

Suler, 'The Online Disinhibition Effect', *Journal of Cyberpsychology and Behaviour* 7/3 (2004), pp.321–6. See also J. Suler, *The Psychology of Cyberspace: The Online Disinhibition Effect*, <http://users.rider.edu/*suler/psycyber/disinhibit.html> (accessed 17 April 2012).

30. J. Bartlett and M. Littler, *Inside the EDL* (London: Demos 2011).

31. انظر:

'Twitterology High and Low', *The Economist*, 31 October 2011, <www.economist. com/blogs/johnson/2011/10/technology-and-language?fsrc=scn%2Ftw%2Fte%2Fbl%2 Ftwitterologyhighandlow> (accessed 16 April 2012).

32. انظر:

'Robin Hood Airport Tweet Bomb Joke Man Wins Case', *BBC News*, 27 July 2012, <www.bbc.co.uk/news/uk-england-19009344> (accessed 16 April 2012).

33. انظر:

'Jack of Kent' (David Allen Green), *Paul Chambers: A Disgraceful and Illiberal Judgment*, 11 May 2010, <http://jackofkent.blogspot.com/2010/05/paul-chambers-disgraceful-and- illiberal.html> (accessed 16 April 2012).

34. انظر:

A. Parker, 'US Bars Friends over Twitter Joke', *Sun*, 30 January 2012, www.thesun.co.uk/sol/homepage/news/4095372/Twitter-news-US-bars-friends-over-Twitter-joke.html (accessed 16 April 2012).

35. انظر:

Intelligence Advanced Research Projects Agency, *Broad Agency Announcement: Reynard Program*, 16 June 2009 <http://www.iarpa.gov/solicitations_reynard.html> (accessed 12 June 2012).

36. على سبيل المثال، في المناطق المحرومة من برلين، تنامى استخدام الموظفين الحكوميين للأجهزة المحمولة المرتبطة بسجلات قواعد بيانات عند زيارة دور الرعاية الخاصة بكبار السن والمستشفيات. توفر مثل هذه الأجهزة وصولاً مستمراً خلال الحركة لقواعد البيانات، ما يمكّن الموظفين الحكوميين من فهم حاجات الأفراد والأسر، ومراجعة الأشخاص الذين يمكن الرجوع إليهم والمشكلات والقضايا الأساسية التي يمكن أن يكون قد تم تسجيلها بوساطة جهات أخرى. انظر:

J. Millard, 'eGovernance and eParticipation: Lessons from Europe in Promoting Inclusion and Empowerment', paper presented to UN Division for Public Administration and Development Management (DPADM) workshop 'e-Participation and e-Government' (Budapest, Hungary, 27–28 July 2006), <unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN023685.pdf> (accessed 23 January 2012).

37. انظر:

Briefing on the Interception Modernisation Programme, *Policy Engagement Network Paper 5* (2009), p.56.

38. انظر:

'Shopping Amid a Massacre: Leaked E-mails from Syria's Regime', *CNN International*, 16 March 2012, <http://edition.cnn.com/2012/03/15/world/meast/syria-al-assad-e-mails/index.html?iphoneemail> (accessed 16 April 2012).

39. للاطلاع على وصف العديد من هذه الاتجاهات، انظر:

Information Commissioner's Office, Information Commissioner's Report to Parliament on the State of Surveillance (November 2010).

40. انظر:

S. Sengupta, 'Zuckerberg's Unspoken Law: Sharing and More Sharing', *New York Times*, 23 September 2011, <http://bits.blogs.nytimes.com/2011/09/23/zuckerbergs-unspoken-law- sharing-and-more-sharing/> (accessed 17 April 2012).

41. انظر:

Twitter, *Privacy Policy*, <http://twitter.com/privacy/previous/version_2> (accessed 17 April 2012); Facebook, *Data Use Policy*, <www.facebook.com/about/privacy/your-info> (accessed 17 April 2012).

42. انظر:

B. Johnson, 'Privacy No Longer a Social Norm, Says Facebook Founder', *Guardian*, 11 January 2011, <www.guardian.co.uk/technology/2010/jan/11/facebook-privacy> (accessed 17 April 2012).

43. انظر:

Attitudes on Data Protection and Electronic Identity in the European Union: Special Eurobarometer 359 (Brussels: European Commission 2010).

44. انظر:

D. Boyd and E. Hargittai, 'Facebook Privacy Settings: Who Cares?', *First Monday* 15/8 (2010).

45. انظر:

European Commission, *Data Protection in the European Union: Citizens' Perceptions* (2008), <http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf> (accessed 17 April 2012).

46. للاطلاع على بحث يتناول تصورات الناس للخصوصية، انظر:

P. Bradwell, *Private Lives: A People's Inquiry into Personal Information* (London: Demos 2010), <www.demos.co.uk/files/Private_Lives_-_web.pdf> (accessed 17 April 2012).

47. انظر:

M. Hick, 'Hague: Governments Must Not Censor Internet', *Huffington Post*, 1 November 2011, <www.huffingtonpost.co.uk/2011/11/01/william-hague-government-internet-censorship_n_1069298.html> (accessed 17 April 2012).

48. انظر:

J.P. Barlow, *A Declaration of the Independence of Cyberspace*, 8 February 1996, <https:// projects.eff.org/*barlow/Declaration-Final.html> (accessed 17 April 2012).

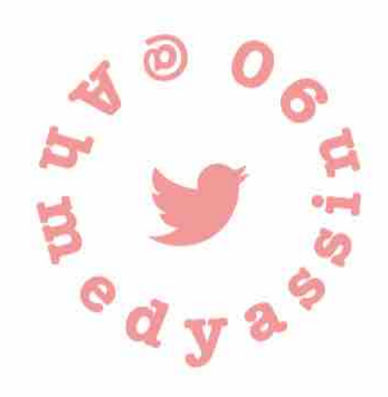
49. D. Omand, *Securing the State* (London: Hurst & Co 2010).

نبذة عن المؤلفين

السير ديفيد أوماند Sir David Omand؛ حاصل على وسام الفروسية، وهو أستاذ زائر في قسم دراسات الحرب في كينجز كوليدج لندن. تم تعيينه في عام 2002 المنسق الرئيسي للأمن والاستخبارات في بريطانيا، وهو مسؤول عن تقديم تقارير لرئيس الوزراء عن الوضع العام لمجتمع الاستخبارات والاستراتيجية الوطنية لمكافحة الإرهاب و"الأمن الداخلي". عمل لمدة سبع سنوات في لجنة الاستخبارات المشتركة. وشغل منصب السكرتير الدائم لوزارة الداخلية في الفترة 1997–2000. وعمل قبل ذلك مديراً لمركز الاتصالات الحكومية. كما عمل لمدة ثلاث سنوات مستشاراً لوزارة الدفاع البريطانية في مقر حلف شمال الأطلسي "الناتو" في بروكسل. تلقى تعليمه في أكاديمية جلاسكو وكلية "كوربس كريستي" بجامعة كامبريدج. نُشر له كتاب بعنوان **تأمين الدولة** *Securing the State* عن دار سي هيرست، بغلاف مقوى عام 2010 وطبعة عادية عام 2012.

جيمي بارتليت Jamie Bartlett؛ هو رئيس برنامج مكافحة العنف والتطرف، ومدير مركز تحليل وسائل التواصل الاجتماعي في مركز ديموس.

كارل ميلر Carl Miller؛ هو شريك في مركز ديموس Demos البحثي، وباحث في المركز الدولي للتحليل الأمني، في كينجز كوليدج لندن.


@Ahmedyassin90

دراسات عالمية

Panton 116 C



استخبارات وسائل التواصل الاجتماعي

السير ديفيد أوماند، وجيمي بارتليت، وكارل ميلر



مركز الإمارات للدراسات والبحوث الاستراتيجية

العدد 125